

Spam Sleuth



©2002-2003 Blue Squirrel, All Rights Reserved

Spam Sleuth Enterprise Administrator's Guide

Spam Sleuth User's Guide

© 2004 Blue Squirrel

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: January 2004

Information in this document is subject to change without notice and does not represent a commitment on the part of Blue Squirrel. The software described herein, including all associated documentation and data, is the exclusive property of Blue Squirrel or its suppliers and is furnished only under a license agreement defining the terms and conditions governing its use by licensee. It is against the law to copy the software except as specifically allowed in the license agreement. No part of this document may be reproduced or transmitted in any form or by any means, including without limitation graphic, electronic, photocopy, facsimile, taping or mechanical reproduction of any kind without the prior written approval of Blue Squirrel.

Use of this product is subject to the terms of the accompanying License Agreement as stated in the back of this book.

U.S. Government Restricted Rights Legend

The Software and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) of the Rights in Technical Data and Computer Software clause at DFARS 52.277-7013 or in subparagraph (c) (1) (ii) and (20) of Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Contractor/manufacturer is Blue Squirrel Software, 686 E. 8400 South, Sandy, UT 84070.

Special thanks to:

All the people that contributed to the development of Spam Sleuth, including the developers, copywriters, web site developers, technical support, customer service, manual editors, alpha testers, the hundreds of beta testers.

Table of Contents

Foreword	0
Part I Introduction and Getting Started	5
1 Installing Spam Sleuth	5
Installation	6
Securing your Installation	6
Master Configuration Files	7
Troubleshooting Installation	7
Check if server is running	7
Check SMTP server	8
Share was not created	8
Lost all Master Users	8
E-Mail not relayed	8
Checking your MX Record	9
2 Configuration - Server	10
Create Share	12
Create Master User	12
Service	13
Access List	13
Advanced Configuration	14
3 Starting Spam Sleuth	14
4 Notifying Users	15
Edit Notify Message	16
5 Configure Your Account	17
Part II Spam Detection Basics	18
1 How Spam Sleuth Eliminates Spam	19
2 Techniques for Eliminating Spam	19
Points System	20
Spam Management	21
Spam Report	21
Part III Configuration	22
1 Configuration of Master Analyzers	22
Accounts (Master)	23
Add/Edit Alias	24
Add New User	25
Active Directory (Master)	26
Active Directory - Edit Domain	27
Friends Master	28
Spammers Master	28
GoodWords Master	28
BadWords Master	28
Attachments Master	28
Dictionary Master	28
Subject Master	28

Power Filter Master	28
2 Configuration of Analyzers	29
Score	29
Friends	30
Mailing Lists	31
Spammers	32
To	33
GoodWords	34
BadWords	35
Profanity	36
Attachments	37
Dictionary	39
Subject	40
HTML Volume	41
Charsets	42
BlackLists	43
HTML Removal	44
Valid Sender	46
Power Filter	48
Bayesian	48
How Bayesian Analysis Works.....	50
Train	51
View Statistics	52
Advanced	52
Turing	53
Turing Test	54
Sample Turing Message.....	55
Advanced	55
E-Mail Stamps	55
Sample E-Mail Stamp Request.....	57
Bouncer	57
Relay	59
Auto Responder	60
3 Mail Jail	61
Drag and Drop	62
Legend for Spam Message Types	63
Right Click Menu	64
Menu	64
File	64
Configure...	64
Export...	65
Exit	65
Edit	65
Delete	65
Delete All	65
Mark as Good (UnSpam).....	65
Mark as Spam	65
Select All	65
Refresh	65
Filter...	65
View	67
Toolbar	67
Status Bar	67

Columns	67
Display	67
View Message	67
Legend	67
Help	67
Help Topics	67
About...	68
Part IV Advanced Features	68
1 Master Files	68
2 Authentication Methods	68
accounts.conf File	69
ldap.conf	70
radius.conf	72
3 domainrelay.conf File	72
4 Learning Mode	73
5 Restrictions	73
6 Score and Store	74
7 Logging	74
8 Server Logging	75
Extended Log Format	76
Common Log Format	76
9 E-mail client relay	76
10 Hidden Server Settings	77
New User Notification	78
11 Command Line Options	79
12 Tips and Tricks	79
Shortcut Keys	79
Positive Tuning	79
Negative Tuning	80
Part V Customer Support	80
1 Spam Sleuth Help File	80
2 How to Find Specific Topics in the Help File	80
3 Visit Our Web Site	81
4 Technical Support	81
5 Customer Service	81
6 Mailing address	81
Part VI Reference	82
1 Glossary	82
2 Appendix A (Regular Expression Syntax)	83
3 Appendix B (Advanced Filter Syntax)	88
4 License Agreement	90

1 Introduction and Getting Started

Welcome, and thank you for choosing the best anti-spam program available.

Spam Sleuth Enterprise will help you win back your e-mail from the scourge of spam (unwanted junk e-mail). Spam Sleuth Enterprise begins removing junk e-mail as soon as you install it and add account information. With a little bit of tuning, you can improve its ability to detect and delete spam from your organization.

Spam Sleuth acts like an e-mail server to the outside world. When e-mail is sent, Spam Sleuth accepts and automatically analyzes e-mail messages for spam characteristics, and when it detects spam, it does not pass it along to your internal e-mail server. Spam Sleuth looks for thousands of different characteristics. It keeps a report of what it finds so that you know exactly why an e-mail has been deemed spam. When Spam Sleuth Enterprise determines an e-mail is spam, the program compresses the message so that it takes as little space as possible on your computer, and keeps a report with the suspect e-mail for a short period of time. After a period of time (30 days by default), it permanently deletes it.

When your e-mail program gets your e-mail, the spam has already been removed and you can read your e-mail the same way you always have, but without sorting through the junk e-mail to find the gems. Spam Sleuth removes the junk for you.

Spam Sleuth Enterprise is a tool for the organization to use to combat spam. Some settings, such as Master GoodWords, Master BadWords, Master Friends, Master Spammers and Master PowerFilter, can set only by Master Users for the entire organization. Other settings can be set by regular end users. The end-users can override most of the master settings if they wish.

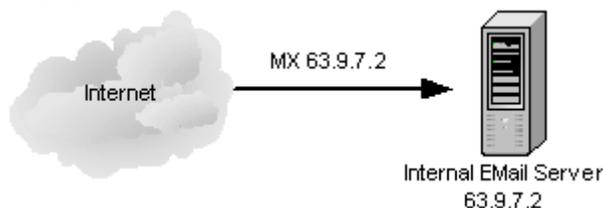
If you are using this tool to protect children, or you just want complete centralized control of what comes into the organization, you can set your users to No Configuration Allowed or No Config - Can't view spam.

In most organizations, the users will be able configure their own Friends and mailing lists, and to set their own spam threshold. Each user can view spam reports, and determine just how aggressive Spam Sleuth Enterprise will be in eliminating spam from their account.

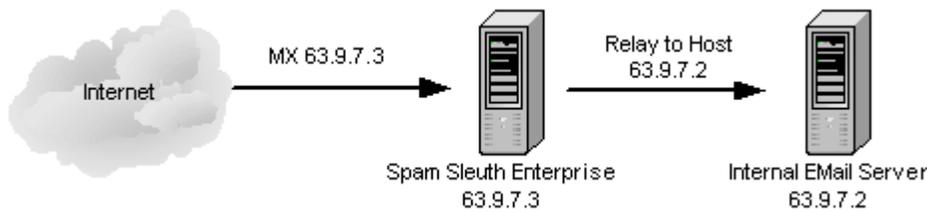
1.1 Installing Spam Sleuth

Spam Sleuth Enterprise should be installed on Windows 4.0, Windows 2000, Windows 2003 or Windows XP. Spam Sleuth Enterprise will act as your e-mail server to the outside world. It will screen e-mail as it comes in. The good e-mail will be forwarded to your internal e-mail server. The spam will temporarily stored and can be viewed by users who have permission.

Before



After



Installation Instructions

1.1.1 Installation

Spam Sleuth Enterprise will only run on a Windows NT, Windows 2000, Windows XP system because it runs as a service.

Steps:

1. Run `SpamSleuthEnterpriseSetup.exe` from the CD or from a download.
2. Specify the location to install the files.
3. After the files have been installed, the Server Configuration will be launched.
4. Spam Sleuth will ask if you'd like to share the directory. You should answer "YES" to create a share that the end-users can use.
5. Set the Relay to Host to the name or IP address of your e-mail server.
6. When you exit the Server Config, it will prompt you to create a Master User. You must have at least one Master User so you can add and edit accounts.

The Install creates three directories:

- \Client - Contains the Analyzers and the Spam Sleuth Client program.
- \Server - Contains the Spam Sleuth Service program and its configuration files.
- \Spam - Contains the Master config files and user spam directories.

For more information on security of these directories, see [Securing your Installation](#).

1.1.2 Securing your Installation

Depending on the type of organization you have, you may wish to secure your installation. You can use the NT Security Model to secure your installation and keep anyone from maliciously changing the configuration, or for the truly paranoid even keep one user from reading another's spam.

Spam Sleuth Enterprise uses three root directories. This is done so that you can secure them at different levels. Please see the documentation for your operating system for information on setting security on folders.

Setting the security to tighter levels of security of the folders is optional, and is not required for Spam Sleuth to function. If you find that Spam Sleuth is not functioning correctly, you may have set the permissions incorrectly. Setting the permissions back to Full Control for Everyone should resume operation.

\SERVER - This directory is only needed by SYSTEM, and anyone who is allowed to configure the server. The `SpamSleuthServer.EXE` runs as SYSTEM by default, but you can change that if you wish. See your operating system documentation for information on changing the Account under which a service runs.

\CLIENT - This directory is used by every user that is allowed to view their spam and configure their preferences. It can be read-only for each user, or group.

\SPAM - The root of this directory contains the MASTER configuration files. The MASTER configuration files must be read-only for all users and read/write for all Spam Sleuth Master users.

\SPAM\

\SPAM\

1.1.3 Master Configuration Files

The Master Configuration Files are the rules for Friends, Spammers, GoodWords, BadWords and Power Filter for the organization. They are shared by everyone in the organization. They can be overridden by any user with configuration ability.

These files are in the root of the \SPAM directory and must be read-only to everyone and read/write for all Spam Sleuth Master users.

1.1.4 Troubleshooting Installation

In most cases the installation is a very smooth and easy process. Here are some things to check if things do not go as expected.

- Check if server is running
- Check SMTP server
- Share was not created
- Lost all Master Users
- E-Mail not relayed

1.1.4.1 Check if server is running

To check if the server is running, you can bring up the task list on the server with CTRL-ALT-DEL and choose *Task Manager* and then the *Processes* tab. You should see SpamSleuthServer.exe running in the task list.

If the service is not running, you should go to the Server Config and hit the Service button and Install or Start the service. If it does not start, check the following:

1. Make sure SpamSleuthServer.exe is in the Server directory.
2. Make sure your operating system is not running older versions of mfc42.dll, msvcp60.dll, msvcrt.dll
3. Try running "SpamSleuthServer.exe /D" from Start->Run. This will run the server in debug mode as a console application.

1.1.4.2 Check SMTP server

To make sure the SMTP server is running, you can telnet to the machine on port 25.

Steps:

1. Go to a command prompt on the server computer
2. Type "Telnet localhost 25" (without the quotes)

You should get back "220 Blue Squirrel SMTP"

If the SMTP server is not running, make sure that you don't have another SMTP server running on port 25.

1.1.4.3 Share was not created

The Server Config will ask you if you would like to create a share when it is first run. If you choose No, it will ask each time you run the Server Config.

The share is used by the end-users to launch <share>\Client\SpamSleuth.exe so they can configure their own spam settings.

If the share is not created by the Server Config, you may not be logged into the server with sufficient rights to create the share. We recommend that you log in with an account that has right to create a share.

You may also create the share yourself. If you do, make sure that you give the server directory the SYSTEM right so that the service can use it. See Securing your Installation for more information on the required rights.

1.1.4.4 Lost all Master Users

When the Server Config exits, it checks for at least one Master User. If it does not find one, it will prompt for one.

Under normal circumstances it would be difficult to lose all of the Master Users, as the Accounts Configuration will not allow you to save without at least one Master User.

If you have lost an employee or contractor that was the sole Master User, you can edit the Accounts.CONF file and set one of the users to *e-mail=1*.

1.1.4.5 E-Mail not relayed

Under normal operation, Spam Sleuth Enterprise will accept all e-mail, get rid of the spam by sorting into a user's folder for pre-view, and forward the good e-mail to your internal e-mail server.

If the e-mail is not being relayed to your e-mail server, you should check the following:

1. Make sure that the name or IP Address is set in the **Relay to Host** in Server Config.
2. If you did use a name instead of an IP Address in **Relay to Host**, make sure the server is able to look up the name. A good way to test this is to go to a command prompt and type "ping *name*" (without the quotes), where *name* is the name you've put in **Relay to Host**.
3. Test your e-mail server by going to a command prompt and typing "telnet *name* 25" (without the quotes), where *name* is the name or IP Address you've put in **Relay to Host**.
4. Check the Accounts to make sure that the user exists, and that the Unknown e-mail is going where you expect it to.
5. Turn on **Log SMTP Relay** in Server Config to log the entire SMTP conversation between Spam

Sleuth Enterprise and your internal e-mail server.

1.1.4.6 Checking your MX Record

E-mail servers send e-mail by first looking up the MX (Mail eXchange) record for your domain name. You can have more than one MX record with different priorities.

Example:

```
MX 10 mail.mydomain.com
MX 20 mail2.mydomain.com
MX 100 backupmail.mydomain.com
```

In the case above, the mail server will send first to the machine mail.mydomain.com by looking up its "A Record" If it is unable to deliver e-mail, then it will try the one with the next priority which would be mail2.mydomain.com, and lastly the backupmail.mydomain.com will be tried.

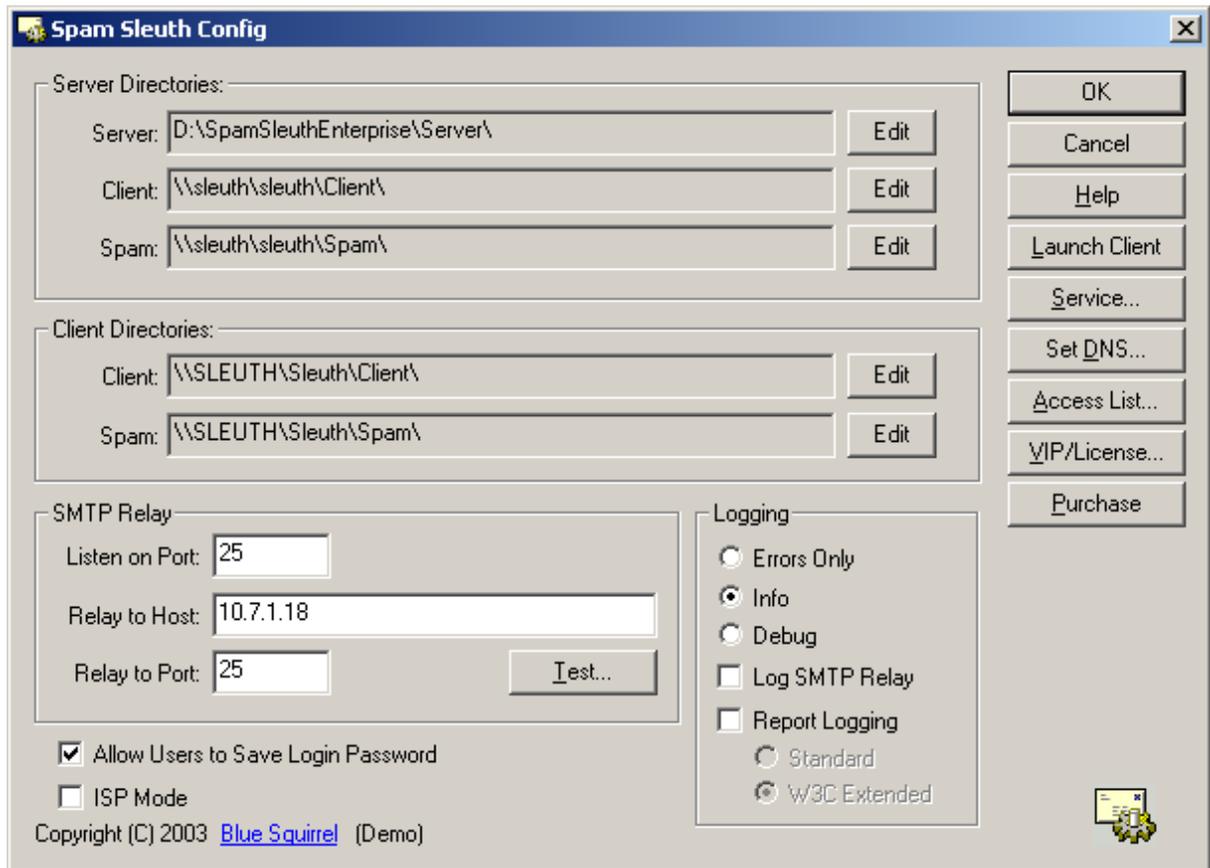
If there are no MX records, the mail servers will use the "A Record" for the domain.

You want to make sure that all your MX records are going to Spam Sleuth Enterprise or to a store-and-forward backup server, which will relay the messages to Spam Sleuth Enterprise when it is available. If you left the IP address of your e-mail server the same, and gave Spam Sleuth Enterprise a new IP address, then you'll need to change your MX records to go to Spam Sleuth Enterprise.

To test your MX records in Windows:

```
NSLOOKUP
>SET TYPE=MX
>mydomain.com
[Lists the MX Records for mydomain.com]
```

1.2 Configuration - Server



WARNING: The SCONFIG.EXE should only be run on the server which runs Spam Sleuth Enterprise as an NT service. Do not try to run SCONFIG.EXE from another workstation.

When the Server Configuration first runs, it will check to make sure there is a valid share for the end-users to access the client directory. If it does not find one, it will ask you if you want to Create a share.

Server Directories - Used by the service

- **Server Directory** - This is the location of SpamSleuthServer.exe and its configuration files.
- **Client Directory** - This is the location of SpamSleuth.exe and the Analyzer modules.
- **Spam Directory** - This is the location of the Master Configuration files, and each user's config files and their temporary spam holding area.

Client Directories - Used by the Windows client

- **Client Directory** - This is the location of SpamSleuth.exe and the Analyzer modules (as seen by the client). This is usually a UNC path so it can be "seen" by the workstations.
- **Spam Directory** - This is the location of the Master Configuration files, and each user's config files and their temporary spam holding area (as seen by the client). This is usually a UNC path so it can be "seen" by the workstations.

Listen on Port - This is the port that Spam Sleuth listens for incoming e-mail traffic. This will almost always be port 25 unless you have a firewall that does port mapping and you choose to run it on a non-standard port inside your firewall.

Relay to Host - This is the name or IP of your e-mail server such as Exchange, IMS, QMAIL, or SendMail.. All non-spam e-mail will be relayed to this server. If you choose to run Spam Sleuth Enterprise on the same computer as your e-mail server, set this to the IP of the computer, but do not use the self-refencing IP of 127.0.0.1, because the client also uses this IP address.

Relay to Port - This is the port that Spam Sleuth will use to send e-mail to your e-mail server. The non-spam messages will be send via SMTP to this port on the computer specified in Host. It will almost always be 25 unless you have chosen to run your e-mail on a different port for security reasons, or to be able to run your e-mail program on the same computer as Spam Sleuth Enterprise.

Logging

Errors Only - Logs errors

Info - Logs information in addition to errors

Debug - Logs Errors, Info, and lots of information that can be used for diagnostics.

Log SMTP Relay - Logs the entire SMTP conversation between Spam Sleuth Enterprise and your internal e-mail server.

Report Logging - Logs information on each e-mail in a standard log format for reporting

- Standard - A simple standard log format
- W3C Extended - An extended log format with more information. See Logging for more information.

Launch Client - Launches the Spam Sleuth client. The Spam Sleuth client lets you configure users, add alias accounts, configure Master users and more.

Service... - Lets you Install, Uninstall, Start and Stop the Windows Service which is the server portion of Spam Sleuth Enterprise. The service must be installed and running for Spam Sleuth Enterprise to accept, scan and relay e-mail. When you exit the Server Configuration, it will check to make sure that the Service is running. If it is not, you will be asked if you want to install/start the service.

Set DNS... - Lets you set DNS entries for the server and the end-users to use. In most cases, the DNS settings that the Windows server is using will be automatically detected and used.

Access List - You can set an access list which will determine which computers will relay, reject or analyze. If you would like your e-mail clients to be able to send e-mail through Spam Sleuth Enterprise to be relayed to your e-mail server. If you are running Spam Sleuth Enterprise on the same computer as your e-mail server, you will need to use the access list to allow your e-mail clients to send e-mail.

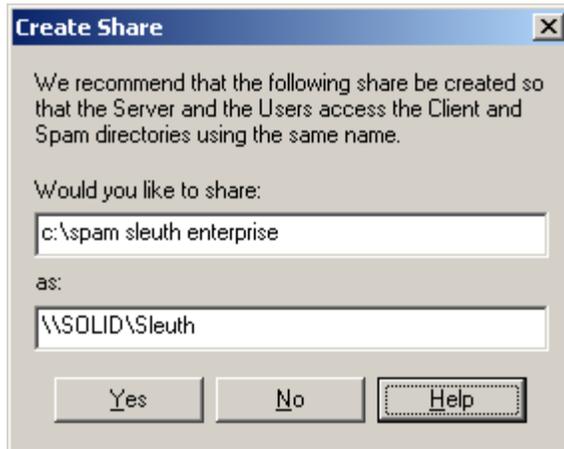
VIP/License - The VIP Key button lets you enter your VIP Key which controls the number of licenses. Each user must have a license.

Purchase - Launches the Blue Squirrel website where you can purchase licenses.

Allow Users to Save Login Password - If this is checked, then the end-users can save their password and automatically log into Spam Sleuth without entering their password each time. You may wish to uncheck this option if you are using LDAP/ActiveDirectory authentication because the password must be stored in the user's registry.

ISP Mode - This is a memory efficient mode which will only load the necessary configurations to analyze the current in-bound e-mails. This mode should be used when there are a large number of users. A guideline would be to use ISP Mode when there are 1000+ users.

1.2.1 Create Share

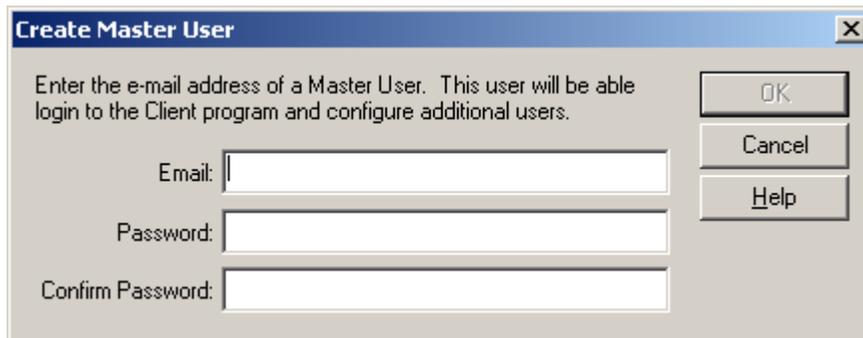


Creates a share that will be used by the server as well as any users who use the Spam Sleuth for viewing their spam and customizing their settings.

The share is created for all **Authorized Users** and for **SYSTEM**. **SYSTEM** is required for the service. **Authorized Users** is for the end-users to connect.

If you choose No, you may still use Spam Sleuth Enterprise, but you will need to create your own share and permissions for users to access the Client directory.

1.2.2 Create Master User



You must have at least one Master User. If the Server Configuration does not detect at least one Master User, you will be prompted to create one.

1.2.3 Service

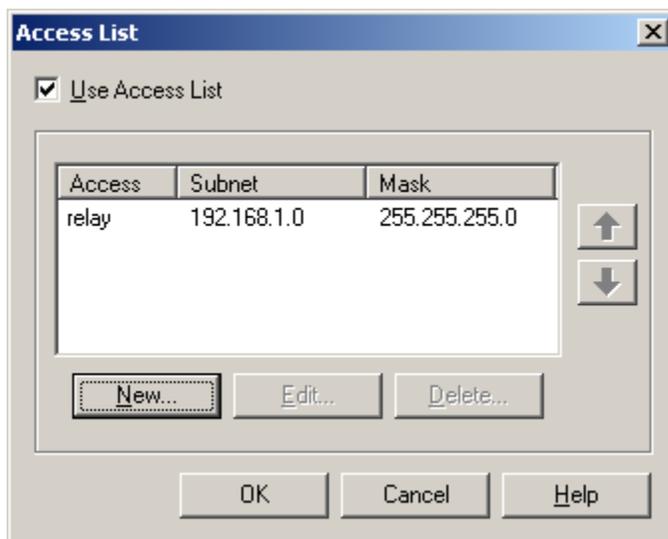


Spam Sleuth Enterprise runs as a service. You can install/uninstall and start/stop the service from the Server Config.

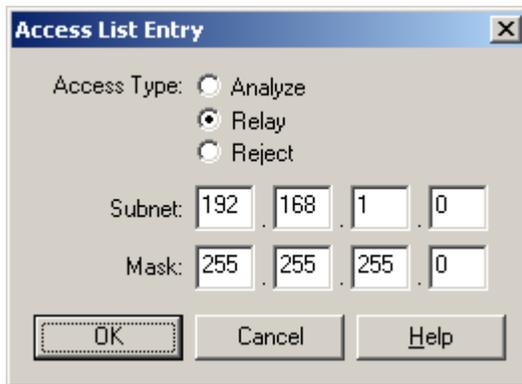
Hitting **I**nstall will install and start the service.

Under normal operating conditions, you should see "The service is running."

1.2.4 Access List



The Access List lets you set up certain IP address ranges which will either be rejected, analyzed, or relayed. You can change the order. As soon as the incoming IP matches a range, then matching will stop. If the incoming IP does not match any ranges, then the default processing will be used. The default processing is to analyze the message if the RCPT TO: of the e-mail matches a valid user/domain.



Analyze - This is the default, and would only need to be used if you needed to set up an ip address or IP range to analyze before an IP address or IP range you are rejecting or relaying.

Relay - This lets you set up a range of addresses from which e-mail will be relayed. Relaying will cause Spam Sleuth Enterprise to relay the message directly to the e-mail server without looking at the domain, or the contents. You should enter the range of your client computers if you install Spam Sleuth Enterprise on the same computer as your e-mail server, otherwise your e-mail clients will not be able to send e-mail without changes to the e-mail client configuration.

Reject - Spam Sleuth Enterprise will reject attempts to connect. You can use this to reject e-mail from blatant abusers of your e-mail system.

1.2.5 Advanced Configuration

If you are an ISP, or an organization with a large number of users, you will want to turn off LoadAndKeep so that you don't over-tax your server's memory.

In the `SpamSleuthServer.INI`, set:
`[General]`
`LoadAndKeep=0`

This option will on-demand load the configuration on an as-needed basis. In this configuration, you can have a large number of users. We recommend that you set this option if you have over 500 users, or if you have over 100 users that are using the Bayesian Analyzer.

1.3 Starting Spam Sleuth

The Spam Sleuth Server runs in the background detecting spam and eliminating it before it reaches you.

If you have been given access, you can run Spam Sleuth on your computer to view the messages that were detected as spam, and if you have been given permission, you may also configure Spam Sleuth to do an even better job at detecting unwanted junk e-mail.

To run Spam Sleuth, you just need to launch `SpamSleuth.exe` from the server location. You may have been sent a welcome e-mail with the location of `SpamSleuth.exe`. If you have, you can run it by going to Start->Run and entering the full path to `SpamSleuth.exe`. It will look something like this `\\SERVER\SLEUTH\SpamSleuth.exe`.

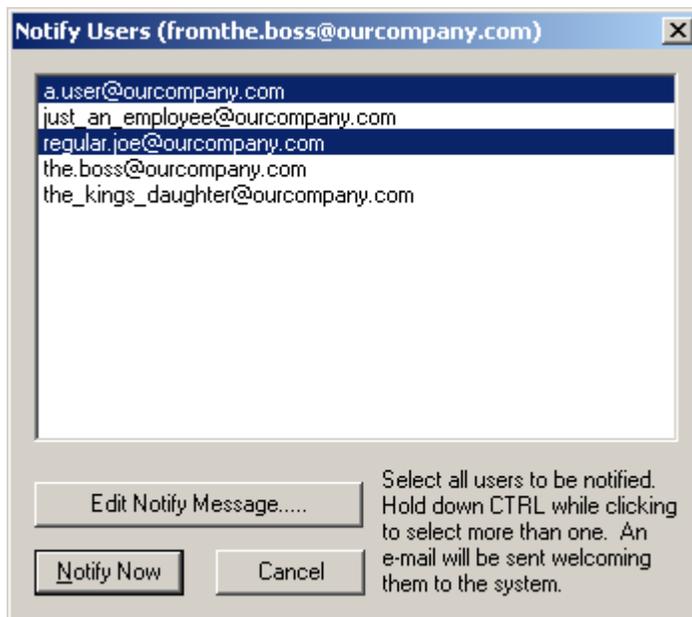
The first time you run Spam Sleuth it will ask for a password. There is a pretty good chance that you don't have a password yet. Just leave it blank and it will take you to Configure Your Account and prompt you to create a new password.

Since you probably don't want to run it that way every time, we have added a check box that lets you put Spam Sleuth right in your Start→Programs.

1.4 Notifying Users

An important step in getting the most out of Spam Sleuth Enterprise is letting users know that this valuable resource exists and is there for them to use. To get to Notify Users, go to Configure..., Accounts and hit the Notify button.

Spam Sleuth Enterprise can e-mail users for you.



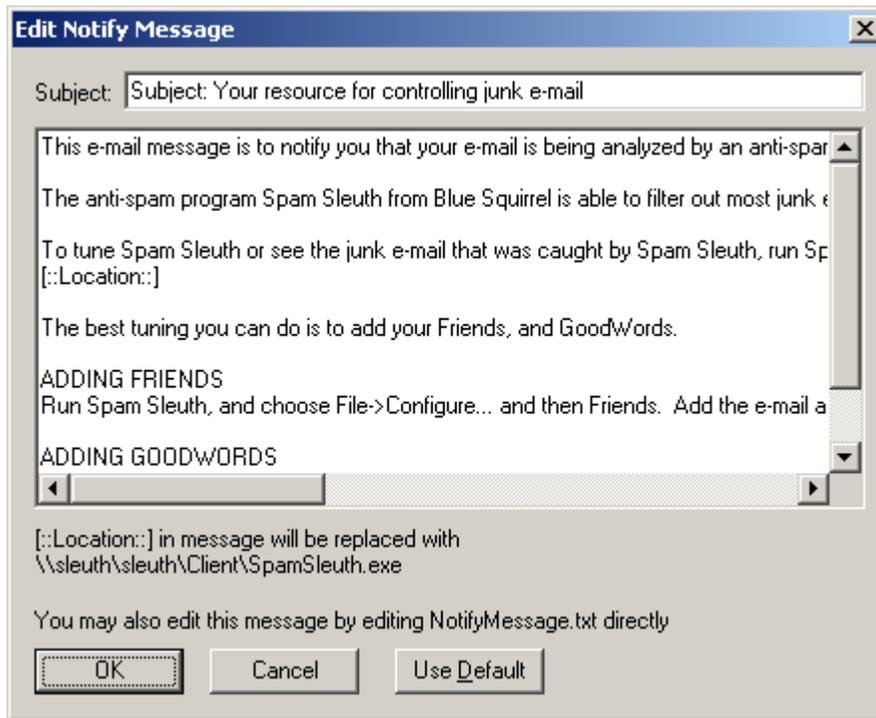
Hitting the Notify button on the Accounts configuration takes you to a list of accounts that are active and have been given rights to use the Spam Sleuth client program to tailor their anti-spam settings.

Select the users you would like to notify. Hold down CTRL to select more than one user.

If you want edit the message that is sent, you can by hitting the "Edit Notify Message" button.

Notify Now will send an e-mail to everyone you've selected.

1.4.1 Edit Notify Message

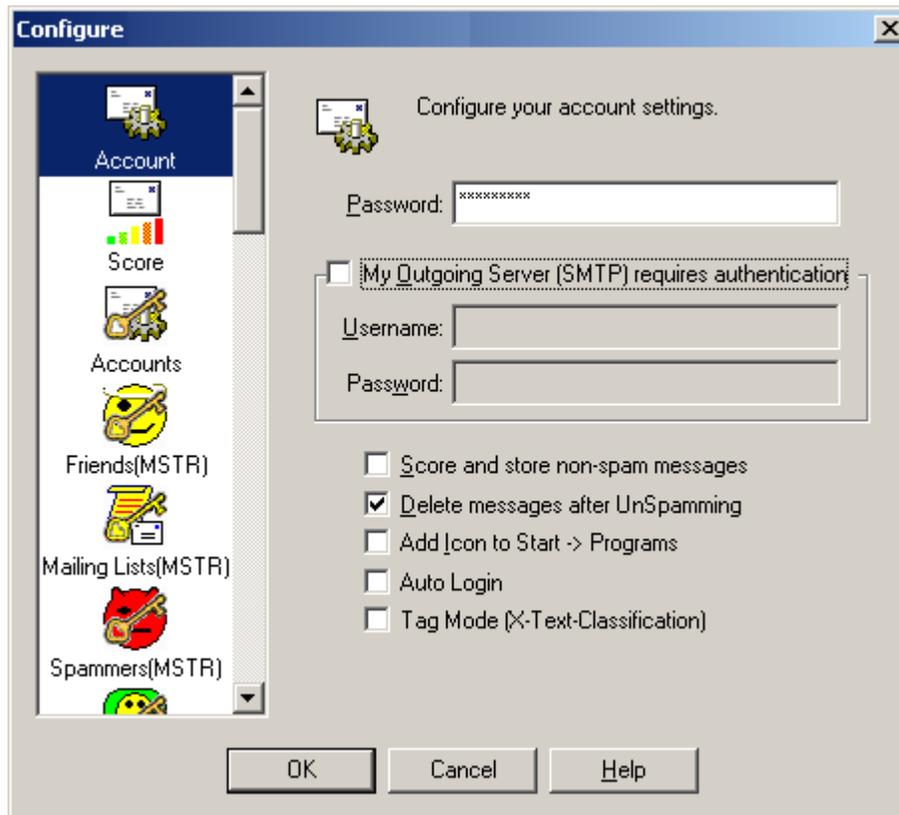


This lets you modify the message that is sent out to users. The message is not sent out automatically, but just to those users you select and hit Notify.

It is recommended that you run SpamSleuth.exe through the same network share that your users will use. This way, Spam Sleuth can detect the location and put the location in the e-mail.

Use Default simply sets the e-mail message back to the default message.

1.5 Configure Your Account



Password - The first time you use Spam Sleuth, you will be prompted to add a password. The password you use does not have to be the same as the password you use for your e-mail. The password is just for the Spam Sleuth viewer and configuring your settings.

My Outgoing Server (SMTP) requires authentication - Set your name/pwd if your company's e-mail server requires a password. Most users will not need to set anything here.

Score and store non-spam messages - Selecting this option will cause Spam Sleuth to keep all of your messages, including ones that were not deemed to be spam. This is useful for tuning, as every message will have a report.

Delete messages after UnSpamming - This causes Spam Sleuth to delete messages from the viewer when you UnSpam and send them back to your InBox. This option is selected by default so that you don't see two messages (one in spam viewer and one in your InBox).

Add Icons to Start->Programs - Adds an icon to the Start menu for conveniently launching Spam Sleuth.

Auto Login - Stores the password and logs in automatically. This option may not be available if your Administrator has disabled the option for security reasons.

Tag Mode (X-Text-Classification) - Adds 'X-Text-Classification: spam' to the header of every spam message so messages can be sorted by your e-mail program. In this mode, all messages are passed through with one of these headers added if the message has been determined to be spam, or has been modified (for script, viruses, etc).

- X-Text-Classification: spam
- X-Text-Classification: modified

2 Spam Detection Basics

The problem of spam is getting worse. Internet researcher Jupiter Media Metrix estimates that consumers will receive about 206 billion junk e-mailings in 2006--an average of 1,400 per person, compared with about 700 per person this year. (Source news.com article March 21, 2002) The same article stated that spam costs "... an estimated \$1 per piece in lost productivity." Although this estimate seems high, spam certainly does waste time and money. Spam Sleuth™ will recover that time and money for you.

The goal is to eliminate spam (or unwanted e-mail) while retaining all the e-mail that you want. Spam Sleuth™ gives you the tools to make this happen. Spam Sleuth does a great job without any configuration except for your e-mail account. It performs even better if you provide it with additional information about what you consider valuable e-mail.

Most friends and business associates that write you letters are not going to have their messages flagged as spam. You may, however, be on some interesting and informative mailing lists that have some spam characteristics. If you let Spam Sleuth know what these are, it will let them right through. Once you've added your mailing lists and most of your friends, you can really crack down on the spam.

Because an occasional desirable message gets marked as spam, Spam Sleuth™ will keep messages so that you can recover them. The default is to keep them for thirty days, but if you're a pack-rat you can keep them longer. Or, you may figure if it is important enough, they'll send it again, and you can have Spam Sleuth™ trash the messages immediately. Spam Sleuth™ will even let you do both, if a message is 'bad enough,' you can have Spam Sleuth™ dispose of it immediately and permanently. But if a message is questionable, you can have it held for you in the Mail Jail.

Each person has their own individual spam tolerance. Some like all real messages to make it into their InBox even if it means some spam may make it in. Some like all spam removed even if it means a few real messages get flagged as spam (as long as they can get those real messages back). We have configured Spam Sleuth somewhere in the middle. It will eliminate 95% of spam, and occasionally a real message will be flagged as spam.

If a message that you really wanted is tagged as spam, you can go to the Mail Jail and read it there in the spam viewer, or you can just "UnSpam" it and it goes right back into your e-mail program.

Spam Sleuth™ goes much further than its "competition" (and we use that term loosely). Spam Sleuth can also remove dangerous attachments, strip out potentially harmful Java™ script, eliminate image links that send your information, and more. Spam Sleuth is pre-configured to remove attachments that can be executed on your computer. All e-mail viruses are spread by sending executable attachments, which Spam Sleuth™ can remove. If you know the attachment is not dangerous, just go to the Mail Jail and "UnSpam" it. Be careful, though, many times the attachments are sent from

somebody you know, but are still dangerous, because your friend didn't send you the dangerous attachment, the virus on their computer sent the attachment.

The folks who send these unwanted e-mails are using tricks to defeat spam programs. Some have even gone as far as encoding the message so that spam programs can't detect key words. Spam Sleuth decodes the messages before analyzing them to counter this underhanded tactic. As new tricks are devised by the spammers, Spam Sleuth will counter them. Spam Sleuth is designed so that new modules can be dropped in and immediately recognized by Spam Sleuth.

Spam Sleuth also uses InstantX™ and Intellimingle™ technology so that it can be updated over the Internet and yet keep all of your settings. You can add your own "BadWords" and the automatic update can update the master list of BadWords also. If you remove one of the words we consider a spam indicator, our updated list will not put it back. Feel free to tailor Spam Sleuth™ to your needs, and allow updates, which keep spam in check.

If an e-mail from a friend or business associate is mistaken for spam, just go to the Mail Jail, right-click and say 'Add to Friends' so that you'll always get their messages in the future and then hit 'UnSpam' to get the message back to your InBox.

More helpful hints for eliminating spam:

- Don't reply to spam messages – then they know you look at your junk e-mail – just add them to Spammers so you don't see their messages.
- Assume that many of the free Internet giveaways are to get your e-mail address. Decide if it is worth it.
- Don't buy anything from spammers – just live without the Flat-Hoses, Viagra, \$50 University Diplomas, and becoming a millionaire this month.

2.1 How Spam Sleuth Eliminates Spam

Spam Sleuth Enterprise acts as an e-mail server to the outside world. When an e-mail comes in, the message is analyzed with the Analyzers and a report is created for the e-mail. If the e-mail exceeds the user's spam threshold, it is compressed and stored instead of being passed along to the organization's internal e-mail server.

2.2 Techniques for Eliminating Spam

Fighting spam is a little bit like fighting computer viruses. It is a constant battle between the Spam detection programs like Spam Sleuth and spammers. We know what some of the spam looks like because we've seen it before, but unfortunately, there will be new things to sell and unscrupulous companies out there that will try to hawk their wares using spam.

Spam Sleuth uses a collection of Analyzers, including: Friends, Spammers, To, Goodwords, Badwords, Profanity, Subject, Attachments, Charsets, HTML Volume, Bouncer, and others to detect and eliminate spam e-mail before you even see the messages. This section of the manual will briefly cover the Analyzers that you have at your disposal, and how to configure them for your needs. For more information about configuring Spam Sleuth's Analyzers refer to the Interface section.

What makes an e-mail spam? Technically, spam is an e-mail that you didn't request, that is commercial in nature and is trying to sell you something or get you to do something. If you signed up for a newsletter, and that newsletter has a sales pitch for the company's product, it isn't technically spam. If you forgot that you signed up, then it sure seems like spam when it arrives.

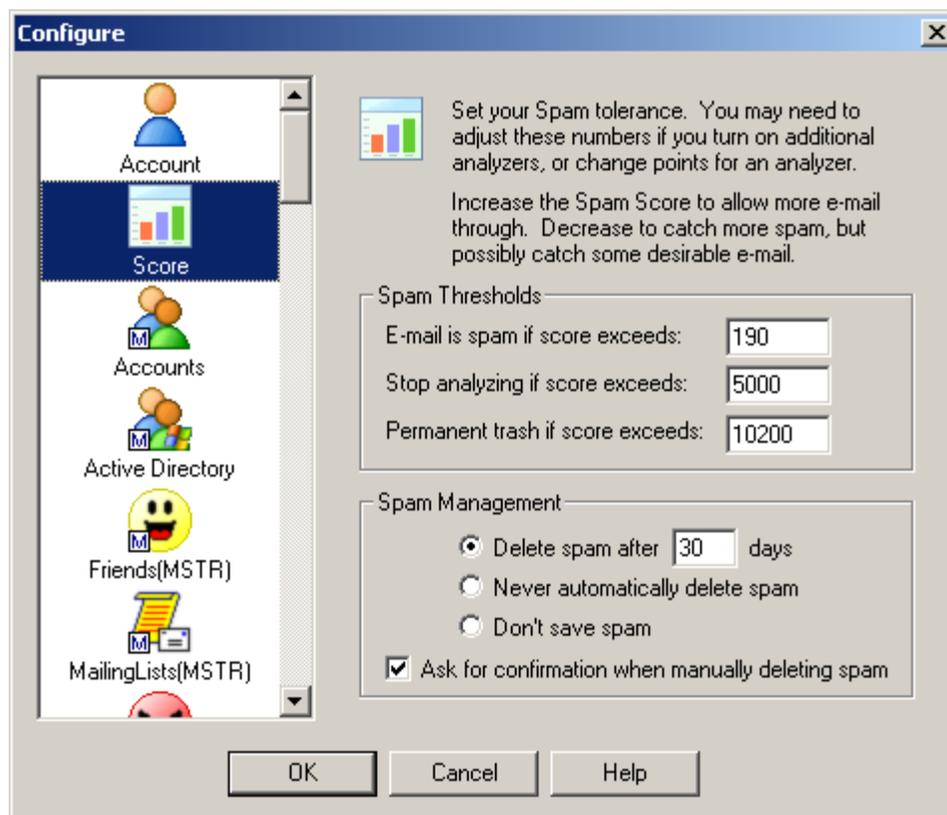
How does Spam Sleuth distinguish between spam and a legitimate newsletter? That is very hard to

do, because the spammers try to convince you that you did sign up with them, or their "marketing partner." Since there isn't currently a way to distinguish the two, we simply define spam as e-mail that you don't want.

2.2.1 Points System

How does Spam Sleuth defeat spam? Each Spam Sleuth Analyzer: Friends, Spammers, To, Goodwords, Badwords, Profanity, Subject, Attachments, Charsets, HTML Volume, etc. looks at your e-mail a different way and can assign points. The more points an e-mail message receives the more likely it is to be deemed as spam. The less points an e-mail message receives the more likely it is a real gem.

Think of it as though it was a contest, and each Analyzer is a different judge, and the messages are the contestants, and Spam Sleuth is the scorekeeper. Every judge looks at the e-mail message and assigns points based on specific criteria. Then all of the points are added together to create an overall total. More points is bad, and less points is good. In the first alpha version of the program, Spam Sleuth sent all the votes to Florida to get a decision, but it always came back a tie and nothing ever happened (only kidding). The number of accumulated points determines if the e-mail message is real, or spam. If the overall total is less than the threshold Spam Sleuth classifies this message as a real gem, and it will be passed through to your e-mail program for viewing. If the overall total exceeds the threshold settings in Spam Sleuth the message is deemed as spam and it will either be placed in the Mail Jail for 30 days, or it will be deleted immediately. Spam Sleuth has 3 different threshold settings that you can adjust to your liking. To configure the threshold settings right click on the Spam Sleuth icon in your Windows System tray > Configure... > Score tab.



- **E-mail is spam if score exceeds:** - If the total amount of points accumulated by all of the analyzers exceeds this number then Spam Sleuth classifies the e-mail as spam, and

the e-mail is sent to the Mail Jail. If you want to see the contents in the MailJail simply double-click on the Spam Sleuth icon. If you don't want to ever see the messages, just wait 30 days and they will be deleted. If the total amount of points is less than this number then this number the e-mail is classified as a real gem and Spam Sleuth will pass the e-mail along to your e-mail program. By default the threshold is set at 190.

- **Stop analyzing if score exceeds:** - The second Spam Sleuth receives e-mail messages the Analyzers begin adding points. If the points begin to exceed 1,000 Spam Sleuth, the scorekeeper, tells all of the analyzers to stop giving points because it is clear that the e-mail message is spam. These types of messages are sent to the Mail Jail, and will be deleted after 30 days.
- **Permanent trash if score exceeds:** - If the overall total of points from all of the Analyzers is more than 10,200 Spam Sleuth immediately deletes the message. These types of messages usually contain adult content/pornography.

2.2.2 Spam Management

Why keep spam for any length of time? Well, there is a chance that a good e-mail will get tagged as spam. Spam Sleuth makes it convenient for you to retrieve good e-mail messages that may have been classified as spam. In the Spam Management section of the Score tab you can tell Spam Sleuth how often to delete messages from the Spam Sleuth Mail Jail. By default Spam Sleuth will delete messages classified as spam after 30 days. As you're looking through the Spam Sleuth Mail Jail you can delete messages at your leisure. By default Spam Sleuth will present you with a dialog to ensure that you want to delete the message. If you prefer not to receive the confirmation message uncheck the **Ask for confirmation when manually deleting spam** check box.

2.2.3 Spam Report

Each message gets a spam report. You can see this report by going to the Mail Jail and double-click on a message. You will see a spam report at the bottom.



Each Analyzer adds its information to the report. The bottom will have a total score for the message.

Show Decoded will show the message after decoding characters and Base64 encoded text. It will not decode attachments.

If you want to see the reports for messages that aren't flagged as spam, you'll need to turn on Score and store non-spam messages in Miscellaneous.

3 Configuration

Most of the time the only thing you'll see is a small icon that sits in your Windows system tray . Once configured, Spam Sleuth™ monitors your e-mail accounts and removes spam before you or your e-mail program sees it.

If you right-click on this icon , you get a menu.



View – Lets you view spam messages in the Mail Jail with a safe Spam Viewer.

Configure... - Brings up the configuration dialog so you can tailor Spam Sleuth™ to meet your needs.

E-mail account list – Choosing an e-mail account will cause Spam Sleuth™ to scan that account for spam.

Email Client – Launches your default e-mail program.

<e-mail address> - Check that account only.

Check All Accounts – Scans all active e-mail accounts for spam.

Exit – Exits the program. Using this Exit will completely shut down the program and Spam Sleuth™ will not be able to prevent spam from getting into your e-mail program unless it is running.

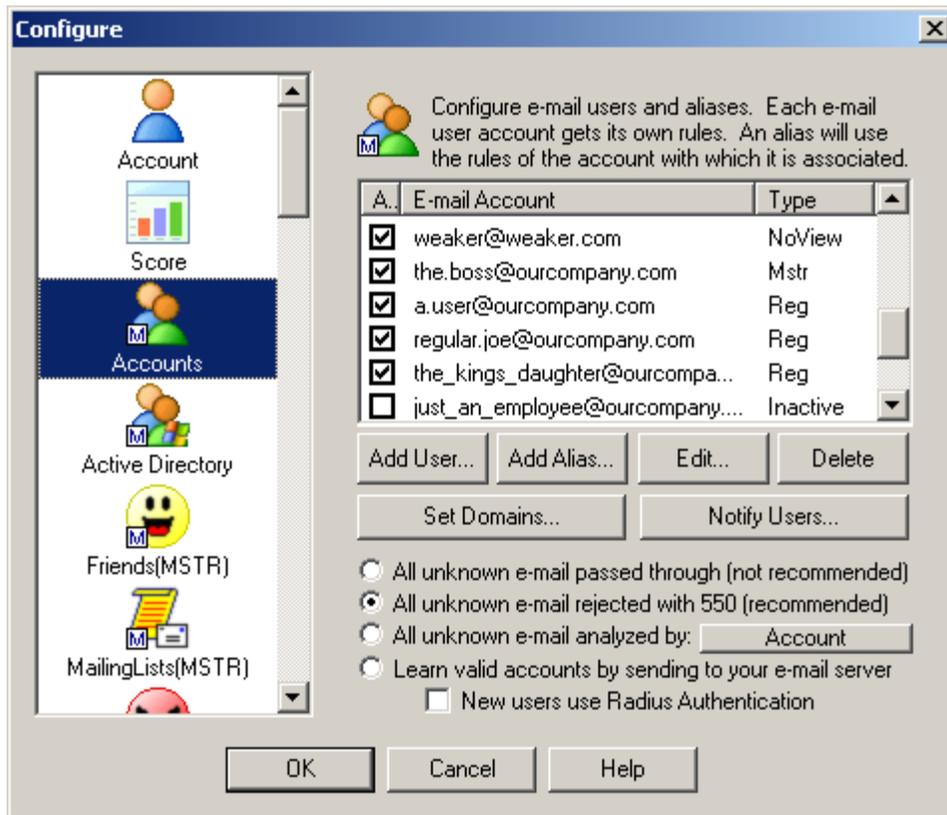
3.1 Configuration of Master Analyzers

The Master Analyzers are only available when Master Users log in. These analyzers are configured for the entire organization. In most cases the users that have configuration control can override the master settings.

Master Analyzers are very useful for medium and large organizations where an IT manager can tune Spam Sleuth for the entire organization.

For example: Say company AlphaWorks owns Spam Sleuth Enterprise and partners with company ZedWorks. A simple addition of *@ZEDWORKS.COM to the Master Friends list will keep all e-mail flowing between the new partners.

3.1.1 Accounts (Master)



Just hit Add New User to add a user account. Spam Sleuth will warn you if you exceed the number of licenses you have purchased, but will continue to let you add accounts. The Spam Sleuth Server will only recognize the first X accounts, where X is the number of licenses you've obtained.

Hit Add Alias to add an alias to a selected account. You must select an e-mail account first. Aliases are just alternate e-mails addresses for their parent account. All e-mail sent to an alias will be analyzed by the rules for the parent account. Spam Sleuth Enterprise is licensed by user, not by alias.

Options

- **All unknown e-mail passed through (not recommended)** - This is OK during testing. Any e-mail that comes in that isn't for one of the user accounts or aliases will be relayed to your internal e-mail server.
- **All unknown e-mail rejected with 550 (recommended)** - This is the best setting for rejecting the spammers. Any e-mail that comes in that isn't for one of the user accounts or aliases will be rejected with a 550 error, which is the SMTP code for "The e-mail account does not exist."
- **All unknown e-mail analyzed [by an account]** - This will route all unknown e-mail addresses to a single account. This is useful when first setting up Spam Sleuth Enterprise to make sure that everyone has an account. You can route all unknowns to the IT administrator so the user account can be added if necessary.
- **Learn valid accounts by sending to your e-mail server** - For accounts belonging to your domain, the program will check with your internal e-mail server by attempting to send a message. See Learning Mode for more information. When learning accounts you have the option to add the new users as RADIUS authenticated users if you have created a radius.conf file. If you have a RADIUS server, the users will authenticate their password against the RADIUS server. See radius.conf for more information. The option will not be available without the radius.conf file.

Edit - This will let you edit the selected user or alias account.

Delete - This will delete the selected user or alias account after confirmation.

Set Domains... - This lets you set your primary and secondary domains. If you set a primary domain, you can add users like *joe* instead of *joe@mydomain.com*. If you add *joe* as a user and you have a primary domain of *pdomain.com*, and secondary domain of *sdomain.com*, the e-mail sent to *joe@sdomain.com* will be analyzed by the rules for *joe@pdomain.com*. Joe will log in as *joe@pdomain.com*, but will get e-mail for both accounts.

For more detail on how to add users programmatically, see *accounts.conf*.

Primary Domain - The primary domain will be used to create the login when only a username is supplied for an account.

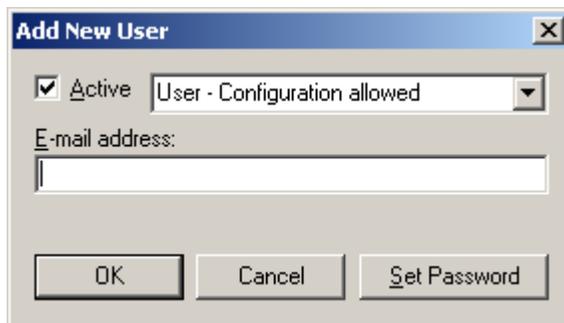
Secondary Domain - The secondary domain will be used to create aliases when only a username is supplied for an account.

If you set at least one domain, then any e-mail sent to a non-valid domain (primary or secondary) will be rejected with a 550 (user not found) error. This is useful, to ensure that your internal e-mail server is not used as an open relay.

Notify Users - This will let you notify users of Spam Sleuth Enterprise and how it can help save them valuable time by removing unwanted junk e-mail.

You must always have at least one active Master user that can get back into the Master configuration to add/edit/remove accounts.

3.1.1.1 Add/Edit Alias

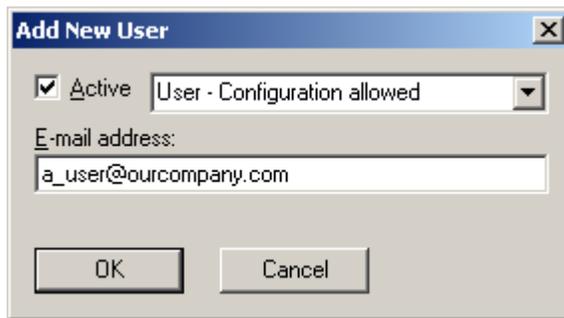


Active - If the alias is not active, the Spam Sleuth Enterprise will not recognize the alias account.

E-mail address - The e-mail address of the alias.

Set Password - Allows the setting of a new user password.

3.1.1.2 Add New User



The screenshot shows a standard Windows-style dialog box titled "Add New User". It features a close button (X) in the top right corner. The main content area includes a checked checkbox labeled "Active", followed by a dropdown menu currently displaying "User - Configuration allowed". Below this is a label "E-mail address:" and a text input field containing the email address "a_user@ourcompany.com". At the bottom of the dialog are two buttons: "OK" and "Cancel".

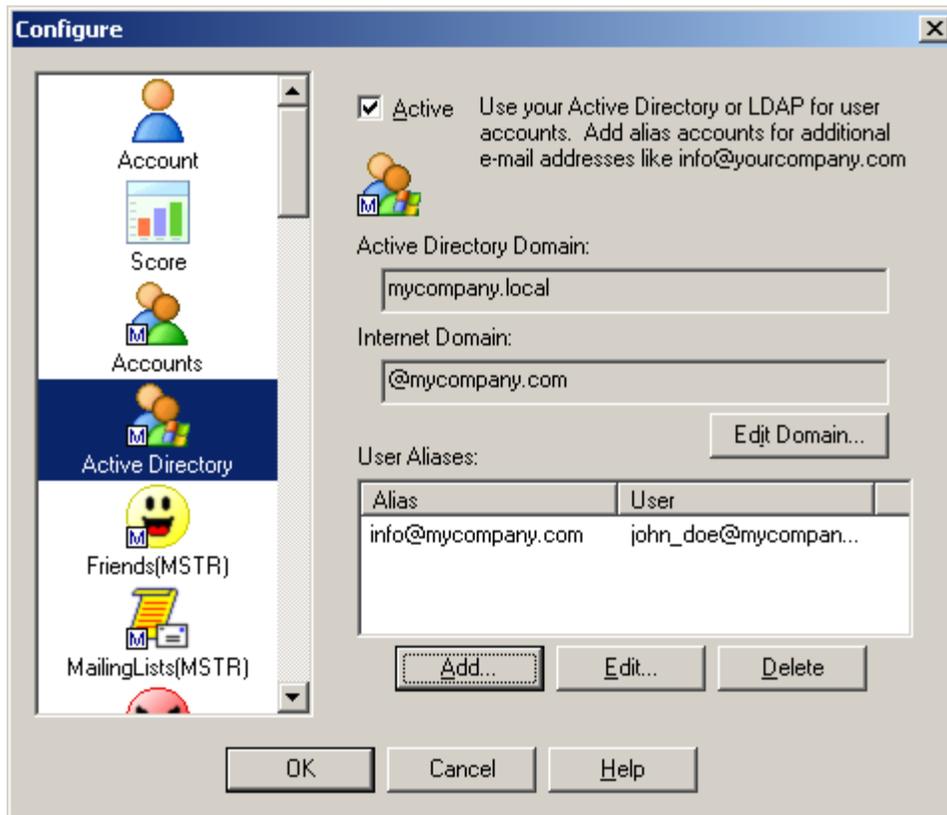
Active - If the user is not active, the Spam Sleuth Enterprise will not recognize the account.

User Types

- **Passthrough Only - No Analysis** - No analysis performed. E-mail is relayed to the internal server.
- **Master User (Master Control)** - Has ability to add/remove accounts and edit all Master Configuration files.
- **User - Configuration allowed** - Can view spam, can configure own spam threshold, and override master files for their account only.
- **User - No Configuration allowed** - Can view spam and retrieve mistaken spam messages, but can't configure settings.
- **User - No Config** - Can't view spam - Can't configure settings, can't view spam. Best option for K-12 school accounts.

E-mail address - The e-mail address for the user.

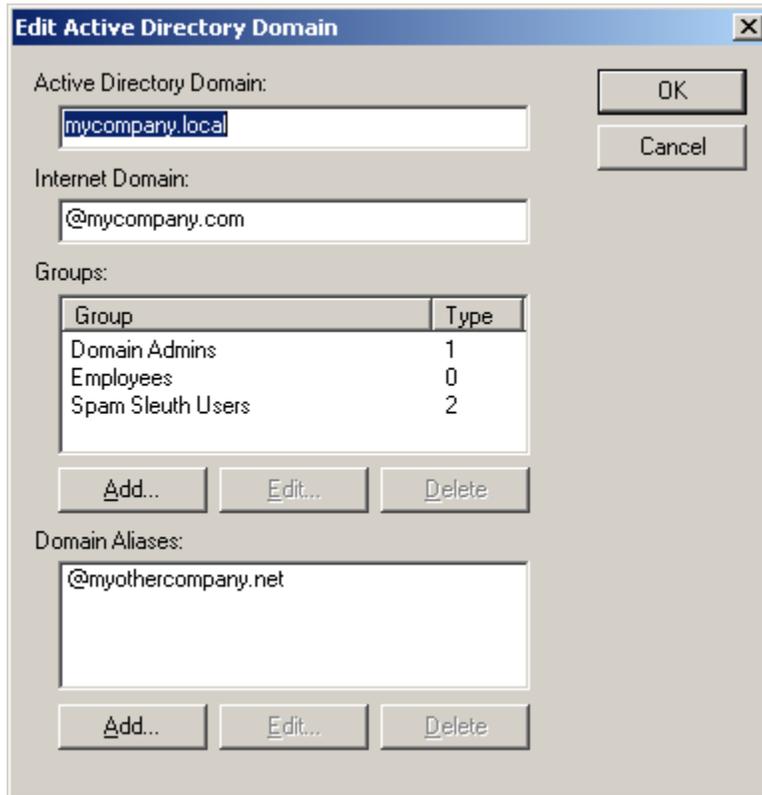
3.1.2 Active Directory (Master)



If you have an Active Directory or LDAP server, you can use it for specifying users and passwords instead of adding them all separately.

First you should hit Edit Domain to set your Active Directory domain and Internet Domain. The members of certain Active Directory groups will become Spam Sleuth Enterprise users. If you have other e-mail addresses that are not users, such as info@mycompany.com, sales@mycompany.com, and webmaster@mycompany.com, you can add those to aliases and specify which user will get the e-mail. Spam Sleuth Enterprise will handle the e-mail routing to get it to the user's e-mail account.

3.1.2.1 Active Directory - Edit Domain



Active Directory Domain - Set your domain here. In many cases it will be the same as your Internet Domain.

Internet Domain - Set your Internet Domain. If your e-mail addresses end in @mycompany.com, then set it here.

Groups - You will set groups that can use Spam Sleuth Enterprise. You set what type of access each group will have. If a user is a member of two or more groups, the user will have the User Type with the most rights.



Domain Aliases - If your users have multiple e-mail addresses, like john_doe@mycompany.com and john_doe@mail.mycompany.com and john_doe@myothercompany.com, then add the other domains here.

3.1.3 Friends Master

The Friends Master list will look exactly like the Friends list, but will apply to the entire organization. Users will see entries that you add here in their own personal Friends list. If they delete these newly appearing entries from their Friends list, the deletion will apply only to their account.

3.1.4 Spammers Master

The Spammers Master list will look exactly like the Spammers list, but will apply to the entire organization. Users will see entries that you add here in their own personal Spammers list. If they delete these newly appearing entries from their Spammers list, the deletion will apply only to their account.

3.1.5 GoodWords Master

The GoodWords Master list will look exactly like the GoodWords list, but will apply to the entire organization. Users will see entries that you add here in their own personal GoodWords list. If they delete these newly appearing entries from their GoodWords list, the deletion will apply only to their account.

3.1.6 BadWords Master

The BadWords Master list will look exactly like the BadWords list, but will apply to the entire organization. Users will see entries that you add here in their own personal BadWords list. If they delete these newly appearing entries from their BadWords list, the deletion will apply only to their account.

3.1.7 Attachments Master

The Attachments Master configuration will look exactly like the Attachments, but will apply to the entire organization. Any entries you make here will also show up in each user's Attachments configuration. The user (if allowed) will be able to override the master Attachment settings.

3.1.8 Dictionary Master

The Dictionary Master configuration will look similar to the user's Dictionary configuration, but will apply to the entire organization. Any entries you make here will also show up in each user's Dictionary configuration. The user (if allowed) will be able to override the master Dictionary settings.

You can edit the Master dictionary, but new dictionary updates would overwrite your dictionary edits.

3.1.9 Subject Master

The Subject Master configuration will look similar to the user's Subject configuration, but will apply to the entire organization. The settings you set here will be the default settings for the user. The user (if allowed) will be able to override the master Subject settings.

3.1.10 Power Filter Master

The Power Filters use individual rules. When you add a rule, it will appear in each user's Power Filter list. If you activated the rule, then it will appear activated in the user's Power Filter rules.

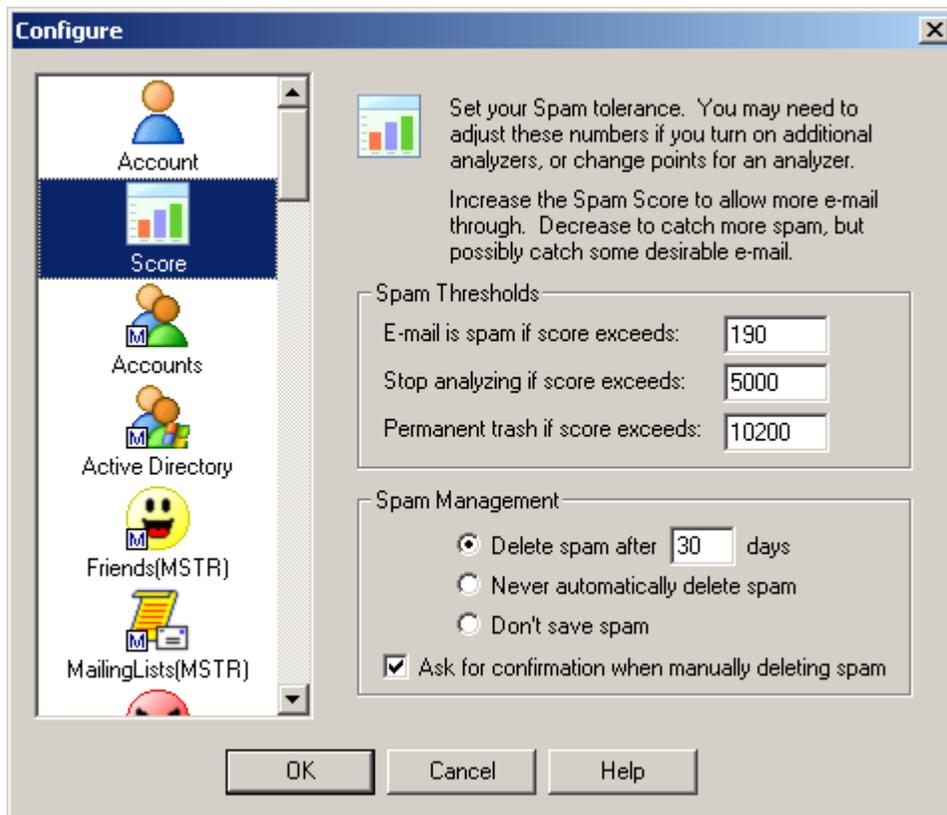
The user can inactivate rules that have been added by Power Filter Master, but they cannot delete them or edit them. They can copy rules and make them their own, and then they can edit them and change the points values.

3.2 Configuration of Analyzers

Each Spam Sleuth analyzer has a different task, and analyzes the e-mail using different criteria. To configure each analyzer right-click on the Spam Sleuth icon and scroll down to the configuration dialog for each analyzer.

The Analyzers are plug-in modules that can analyze an e-mail, assign points, contribute to the spam report, and act on the e-mail if necessary.

3.2.1 Score



Spam Threshold

The Score dialog lets you set your personal spam tolerance threshold. Start with the default settings. Then look at the spam that was caught and the spam that wasn't in the Mail Jail. If you are getting too much spam in your InBox, decrease the spam threshold. If you are losing too many real messages, increase the spam threshold.

Stop Threshold

To be more efficient, Spam Sleuth™ can stop analyzing if the Spam Score exceeds a certain level. If you don't have any *GoodWords* or *Bayesian* then you can set this to the same value as the Spam Score. *Good Words* and *Bayesian* can deduct points from the spam score to allow an e-mail through which may pertain to something you want. If the spam score gets too high, then the *GoodWords* aren't going to help, you may as well let Spam Sleuth™ quit analyzing.

Trash Threshold

If the Spam Score gets too high, there may be no reason to even keep the message in the Mail Jail.

If it is such blatant junk spam, let Spam Sleuth permanently delete it. If you don't like storing any spam, just set the Permanent Trash Score lower than the Spam Score. If you never want to permanently trash e-mail, set this to the highest level of 999,999.

Spam Management

The spam will keep on coming, but you probably don't want to keep it forever. Spam Sleuth does compress the messages so they take less room on your computer. Spam Sleuth will permanently delete spam after so many days. You decide how long to keep it in storage. We've set the default to 30 days, but you might only want to keep it for 5 days. Once a day, Spam Sleuth will clear out messages that are too old to keep. If you lower this number and the spam doesn't immediately disappear, don't worry, wait a day and Spam Sleuth will clean out the old spam.

You also have a choice to never delete spam. We don't recommend this option because spam will just take up your computer's resources.

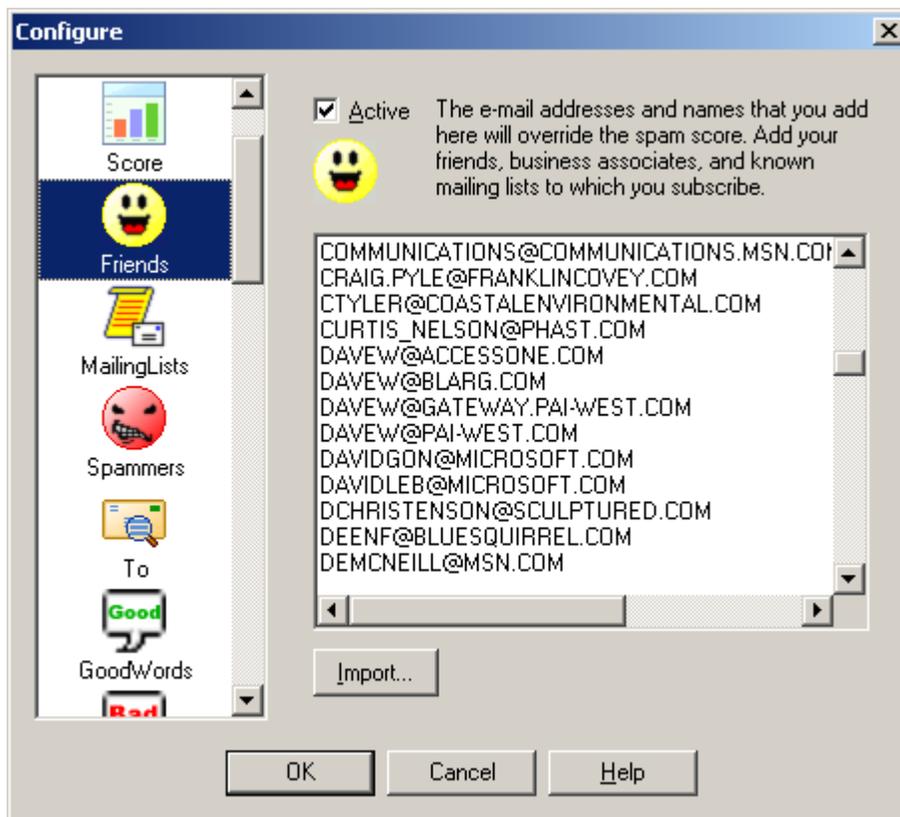
You can choose to never keep spam. We don't recommend this option because if Spam Sleuth mistakenly flags a good message as spam, you will not be able to recover it. If you don't keep spam for some short period of time, you cannot train *Bayesian*, use *Turing*, or *EMail Stamps*. If you are using Tag Mode, you may want to select the option to not keep spam, as all the spam will passed through to the client with a tag identifying it as spam. In this case, the messages can be recovered from the e-mail client if the messages were moved to a Junk folder by the e-mail client's rules.

Spam Sleuth will ask for confirmation when deleting spam, unless you uncheck *Ask for confirmation when manually deleting spam*.

3.2.2 Friends

How can you make sure a message from a friend, relative, or co-worker is not tagged as spam? Spam Sleuth has an analyzer called Friends, which overrides all of the other analyzers. If the e-mail address of your friend is listed in the Friends Analyzer, it will let messages right through to your e-mail program.

What if I don't want to add everyone in my whole company to my friends list, but I want to get their e-mails? That is easy, simply add a wildcard friend to the Friends Analyzer. Use the * to represent any number of characters. Adding *@mycompany.com will let e-mail messages from joe_shmoe@mycompany.com and jane.doe@mycompany.com right through to your e-mail program.

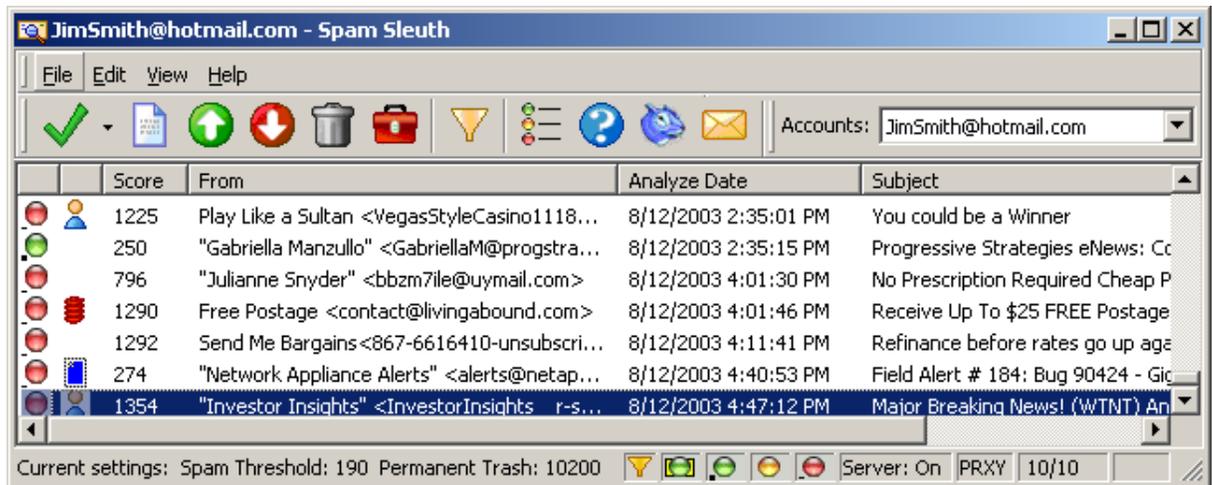


The Friends dialog lets you add e-mail addresses for your family, friends, co-workers and mailing lists. If someone in this list sends you an e-mail, Spam Sleuth will route the message directly to your e-mail program. Spam Sleuth will still strip off dangerous attachments, but you will get the e-mail. Add as many e-mail addresses as you'd like. E-mails are not case-sensitive, so don't worry if the letters are all capitalized.

Friends supports limited wildcards. You can put a * at the beginning or end of a word. Example: *@BLUESQUIRREL.COM would allow all Blue Squirrel addresses that end in @BLUESQUIRREL.COM. You cannot add *@*.DOMAIN.COM.

3.2.3 Mailing Lists

How can you ensure that you get e-mail from certain mailing lists while rejecting ones for which you aren't subscribed?



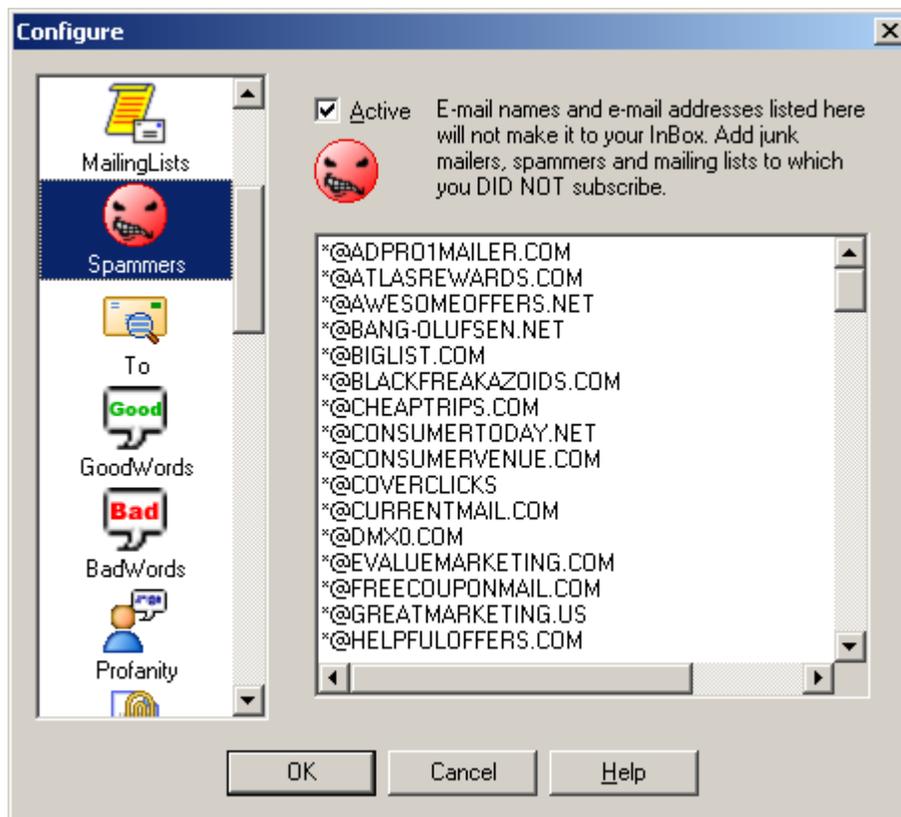
Mailing Lists lets you by-pass the analysis for the mailing lists for which you have subscribed. It is very similar to Friends, but will also check if the To: matches the mailing list name.

Often times, the From: is someone you've never heard of, but they're sending to you by sending to the mailing list distribution system. The To: is usually the e-mail address of the mailing list.

Add your mailing lists here.

3.2.4 Spammers

What if I keep getting e-mails from the same person or company and I don't want them anymore? Just add them to the Spammers Analyzer. This analyzer overrides all analyzers except for the Friends Analyzer. Just add the e-mail address of the person or company and they go straight to the Mail Jail. Use wildcards to eliminate all e-mail from a company.



List all the e-mail address of known spammers. If you don't want to see another e-mail from someone, just add their address to this list. Use the '*' to remove an entire range of e-mail addresses. Put in '*@BADCOMPANY.COM' to block all e-mail addresses with @BADCOMPANY.COM in them. E-mails are not case-sensitive, so don't worry if the letters are all capitalized.

Spammers supports limited wildcards. You can put a * at the beginning or end of a word. Example: *@BLASTMAIL.COM would block all e-mail addresses that end in @BLASTMAIL.COM.

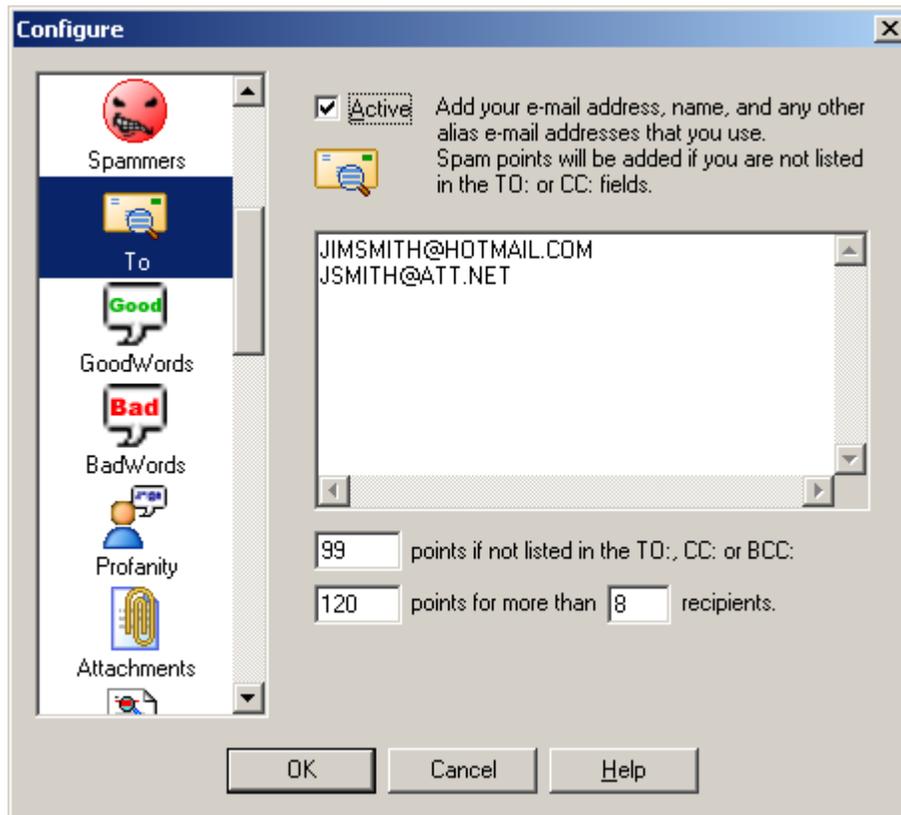
To block e-mails that use various subdomains, like out@mailout.blastmail.com, or out@outgoing.blastmail.com, etc., then you can add *BLASTMAIL.COM to the Spammers list to catch all of them.

3.2.5 To

What if you want to make sure that the sender really knows who you are? Use the **To Analyzer** to filter out e-mail that is sent to "Homeowner", "Resident", or "Potential Customer." Just list all of your real e-mail addresses. Sometimes you have aliases – add 'em to the **To Analyzer** list. For example, if you have multiple e-mail addresses such as bob_jones@mycompany.com and support@mycompany.com that you receive e-mail from then add them to the list.

Have you ever gotten an e-mail with a truck-load of e-mail addresses listed in the *To:* section? Sometimes these are jokes that people are sending to everyone on their address list. Unfortunately, most of the time you are just one of the millions that have been spammed. The **To Analyzer** will count up how many people got the same message. If there are too many then Spam Sleuth will assign some points. You can decide how many people is too many, and you can decide how many

points to assign to the message.



The To list should contain all the valid e-mail addresses for you. If the message is not addressed to one of your e-mail addresses, then it will get spam points. Often unwanted e-mail has ten or more people listed in the To: or CC:. Spam Sleuth™ can assign points for this. You decide how many people is too many, and how many points.

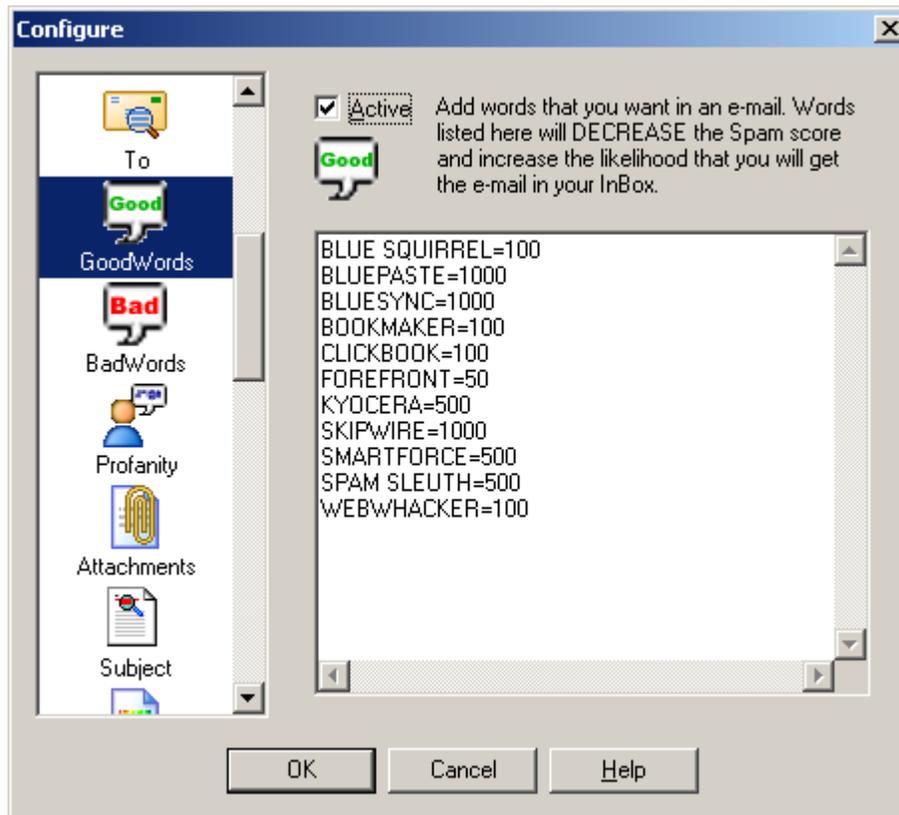
You may be wondering how the message could get to you without your e-mail address being listed. The server that sent it specified that it was for you, but the text of the message which you see (To: joe@xyz.com) can be anything and does not have to list your name. Often times it is more efficient for a spammer (who may be sending millions of message) to make one message and blast it out and have other servers deliver them. Just like when you get junk regular mail at home addressed to "Resident", the To: address might contain something generic like "Homeowner."

The *To Analyzer* supports limited wildcards. You can put a * at the beginning or end of a word. Example: *@MYCOMPANY.COM would accept all e-mail addresses that end in @MYCOMPANY.COM.

3.2.6 GoodWords

Do you sometimes get e-mail that looks like junk, but it really is a good e-mail because it is about something you care about? Maybe you care about basketball, or basket weaving. Everyone has his or her own hobbies and interests. If you put those words in the **GoodWords Analyzer**, it will deduct points when it finds your interests. If you want to see all e-mails about racing, you may want to add "FINISH LINE=1000", "RACING=1000", and "RACE*=1000", remember the * acts like any number of characters. Adding these to the **GoodWords Analyzer** will deduct 1000 points when it finds these

words. Don't forget to add words that pertain to your job.



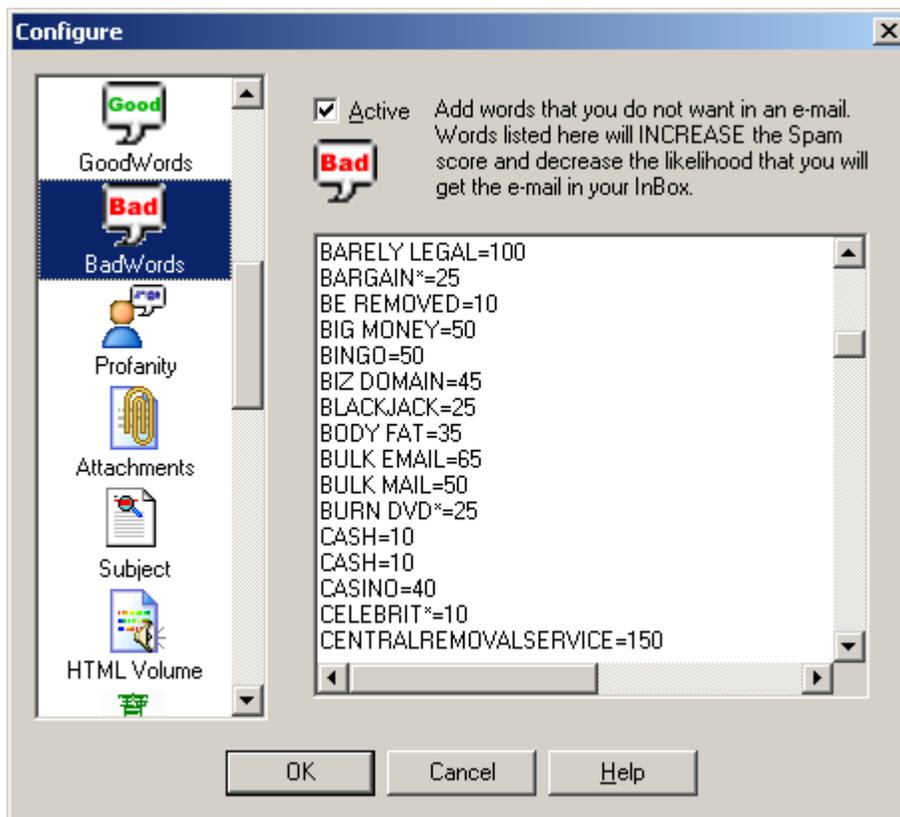
GoodWords let you catch e-mails that may interest you. At Blue Squirrel we have a number of products. If our product names are in the e-mail, we probably want the e-mail even if it has some spam characteristics. The GoodWords will be different for everybody. You might put in sports, or hobbies that interest you, so that you don't miss a good e-mail. You put in the number of points to SUBTRACT from the Spam Score. A high number will ensure that you get e-mails about that subject.

GoodWords will search the entire message, including the header (with the subject).

GoodWords supports limited wildcards. You can put a * at the beginning or end of a word. Example: MINI CAR* would match all words like "Mini Car", "MINI Cars", "mini CART"

3.2.7 BadWords

Do you get e-mails about flat hoses, \$50 University Diplomas and other useless junk? Well we've added a list of words and points to the **BadWords Analyzer**. The **BadWords Analyzer** will catch a lot of junk e-mail. Feel free to add your own words, and remove some of ours. Change the points if you'd like.



BadWords are words that are likely to appear in unwanted e-mail. To add to the list, just enter your word followed by '=', followed by the number of points to assign for that word. Spam Sleuth comes with a list of words that is periodically updated. You can remove words, or add words to this list. Intellimingle™ will automatically add your words to the Spam Sleuth master list of words. If you remove a word, Intellimingle™ will remember that you've removed that word so that when we update the master BadWord list, Spam Sleuth™ won't analyze for the removed word. Feel free to customize this list. If you feel that you will never get a real e-mail about "SuperBiz" then feel free to boost the points for that word to 1000.

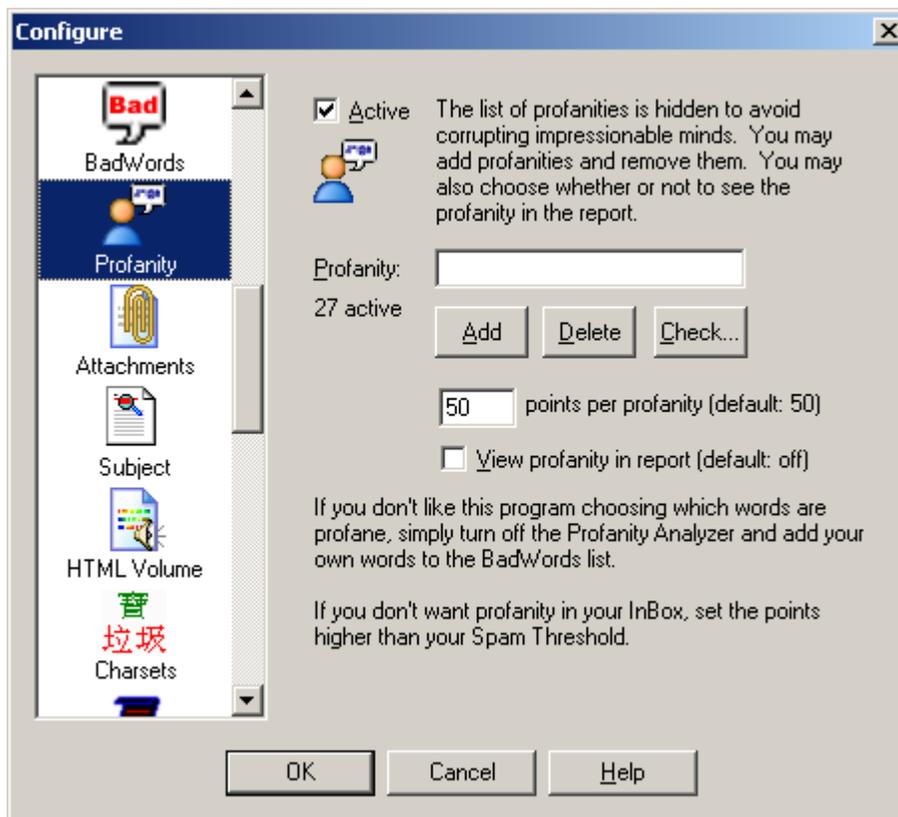
BadWords will search the entire message, including the header (with the subject).

The really profane words are in the Profanity Analyzer.

BadWords supports limited wildcards. You can put a * at the beginning or end of a word. Example: MINI CAR* would match all words like "Mini Car", "MINI Cars", "mini CART"

3.2.8 Profanity

Are you afraid that some really profane e-mails will be seen by your kids? If you have kids you may want to really increase the points in the **Profanity Analyzer**. We have added several words for you, and you can add your own words as well. No worries, the Profanity Analyzer doesn't list the words so you don't have to worry about them being seen by innocent young eyes.



The profanity analyzer looks for the really profane words. We chose not to let you see the list of profanities. If you want to know whether one is in there, you can type it in and hit the Check... button. It will tell you if it is in the list. The data file is encoded, so don't bother looking in there either.

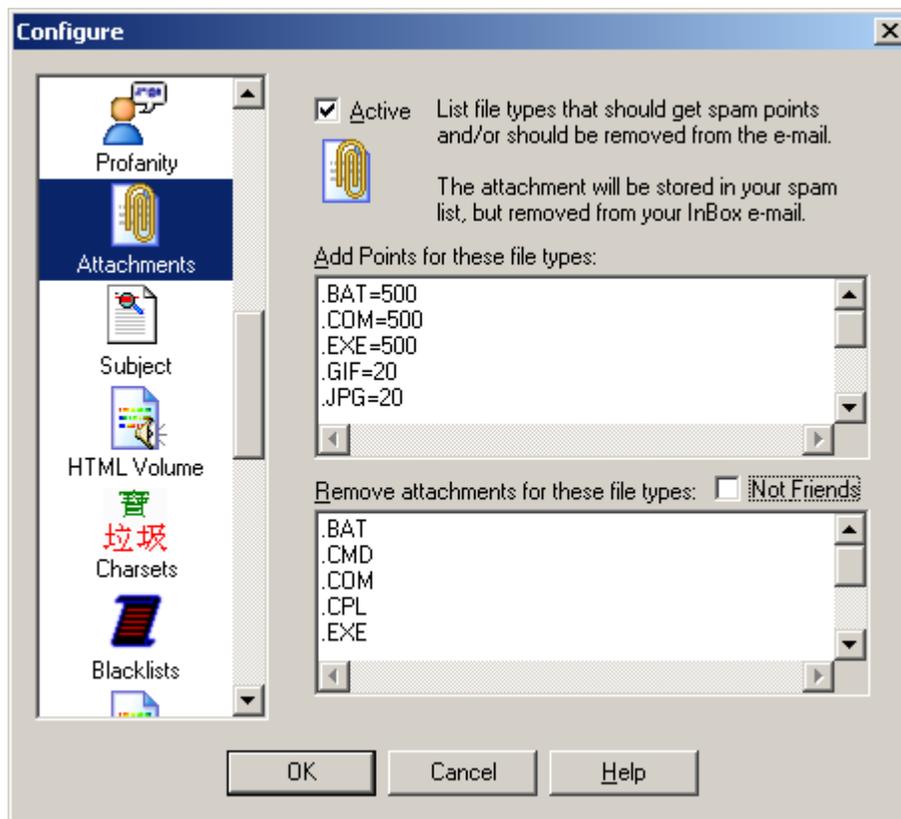
You can add profanities to the list, and you can delete them from the list if you know what they are.

If you want to see the profanity in the Sleuth's report, just check View profanity in report. If you leave it unchecked, you will just see 10 Profanity - '----' The number of dashes represent the number of characters in the profanity. The rest is left to your imagination.

When you set the points, you are setting the points for all the profanities. If you are using Spam Sleuth™ to protect children, you may wish to set this number very high to make sure profane e-mails are relegated to the Mail Jail.

3.2.9 Attachments

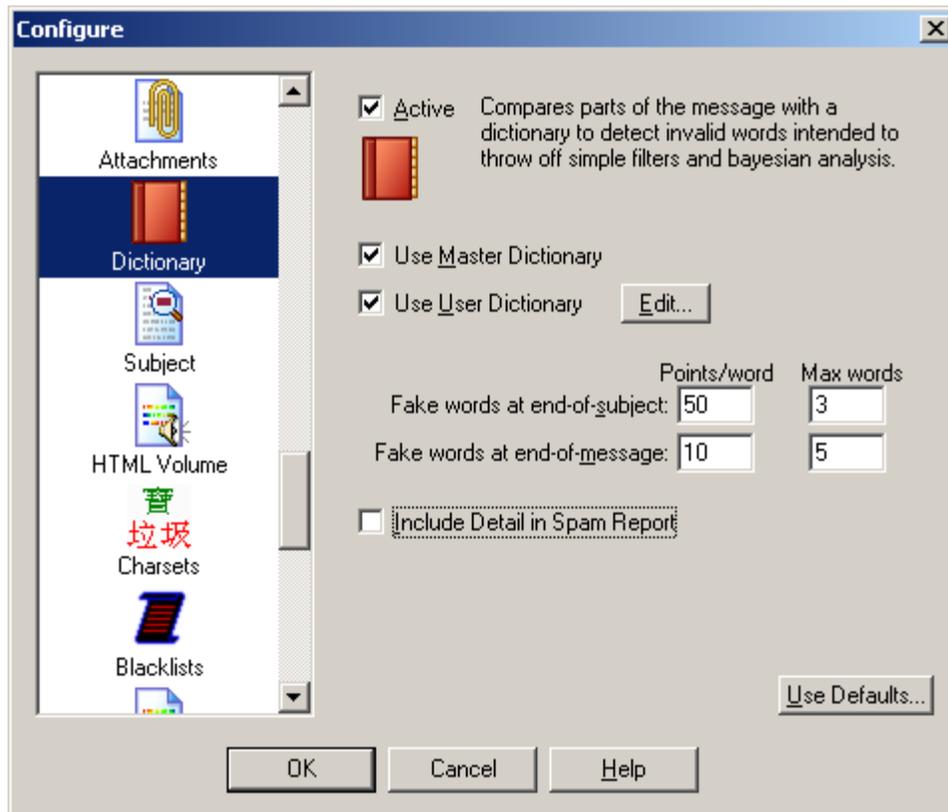
Did you know that all e-mail viruses are spread by sending attachments that can be executed? The **Attachments Analyzer** removes dangerous attachments, such as .exe files. Don't worry it stores the entire e-mail along with the attachment in the Mail Jail if you need it back. Be very careful. Most e-mail viruses are accidentally sent by friends or associates that have you in their e-mail address book. The virus spreads itself by sending an e-mail to everyone in the address book. If you get e-mails with .JPG attachments that are often spam, you can assign 50 points by just adding the line ".JPG=50" to the top box in the **Attachments Analyzer**.



The Attachments analyzer has the ability to assign points, and it also has the ability to remove the attachment. Attachments are dangerous when they are programs that can do anything to your computer. Executable files (.EXE, .VBS, .CMD and others) attached to e-mails are very often viruses. By default Spam Sleuth™ is configured to remove executable files. You can always get the original file back (with attachment) by going to the Mail Jail and hitting "UnSpam." Be careful, often times an executable file that looks like it came from a friend was actually sent by a virus reading your friend's e-mail address book and sending everyone a copy of itself. Unless you've spoken with someone about a file they are sending you, we recommend that you don't run any e-mailed executable attachment.

Checking *Not Friends* will keep Spam Sleuth from removing attachments from e-mails sent from your list of Friends and your Mailing Lists. Before choosing this option, please be aware that viruses are sometimes sent by friends unintentionally if their computer has been infected with a virus.

3.2.10 Dictionary



The Dictionary analyzer uses an English dictionary to determine whether the words at the end of the subject and the end of the message are real. Many spam messages use random letters at the end of the message or the subject to throw off simple filters and Bayesian analyzers. The Dictionary analyzer detects these random letter sequences and assigns them points. You may wish to turn this off this analyzer if your primary language is not English.

Use Master Dictionary - Use the Master dictionary. You should leave this checked unless you are in a non-English speaking country.

Use User Dictionary - Also checks for words in the user's custom dictionary. Use this to add words that are not in the Master Dictionary. [Edit...] lets you create/edit a personalized dictionary file. If you expect e-mails to have certain words at the end, you should add those words to your own personal User Dictionary.

Fake words at the end of subject - By default, the last three words of a subject are analyzed and 50 points per non-word is added to the total score.

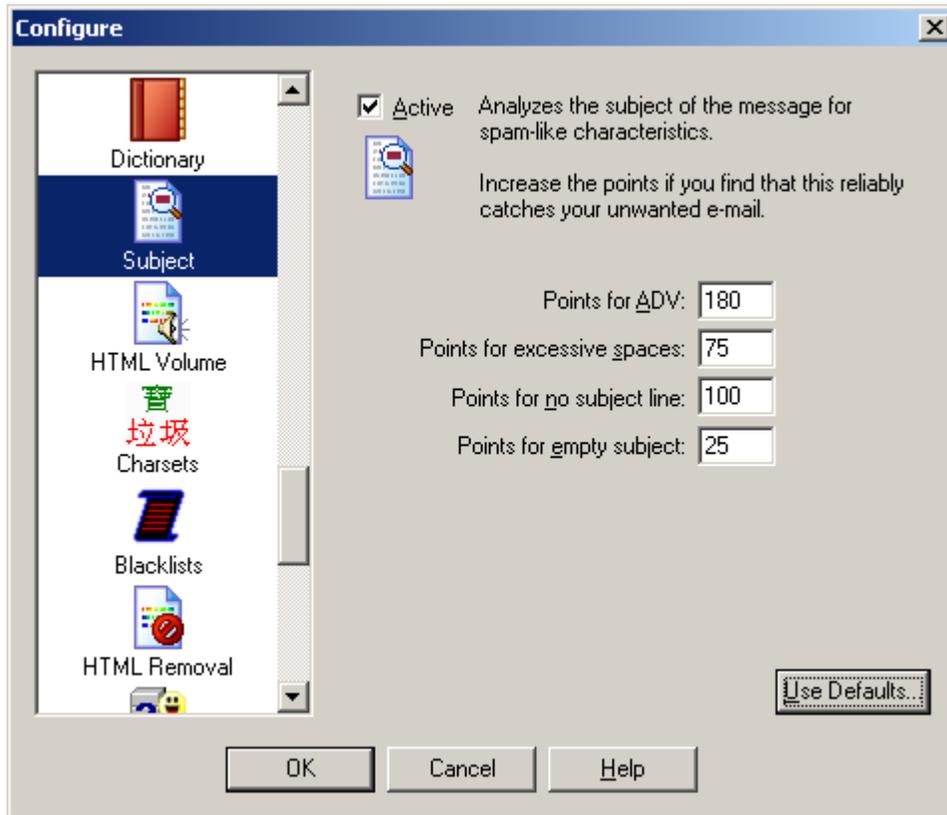
Fake words at the end of message - By default, the last two words of the message are analyzed and 10 points per non-word is added to the total score.

Include Detail in Spam Report - Selecting this option will add additional lines to the spam report that show you which words were analyzed and whether or not they were in the dictionary.

Use Defaults... - Sets Dictionary settings to the defaults.

3.2.11 Subject

Can you identify spam with a single glance at the e-mail's subject? The **Subject Analyzer** looks at the spacing, capitalization, and looks for the legally required, but rarely used "ADV" (Advertisement) to determine whether a message is spam. Spammers also use tricks so that it is more difficult for large ISPs to screen out spam by just the subject. They tack on a unique sequence of letters or numbers to the end of the subject so the subject is always different for each message. The **Subject Analyzer** also looks for that little trick.



The Subject analyzer looks at spam-like characteristics of the subject of a message. You can change the maximum number of points that this analyzer can contribute to the total score. Very seldom will a subject be blatant enough to warrant the maximum score.

Points for ADV - The text 'ADV:' is supposed to appear on advertising e-mails. If everyone did this like they are supposed to, there would be no need for Spam Sleuth. For the few that do, this quickly catches them as spam.

Points for excessive spaces - This catches e-mails with a 'trick' subject. The spammers will tack on some random letters at the end of a subject to keep simple subject filters from filtering them out. Since they put these letters at the end of the subject, there is an excessive number of spaces between the real subject and their little 'trick.' This assigns points for that trick.

Points for no subject line - Set the points that will be assigned when a message has no subject line in the header. This is rare, but does happen with some spam.

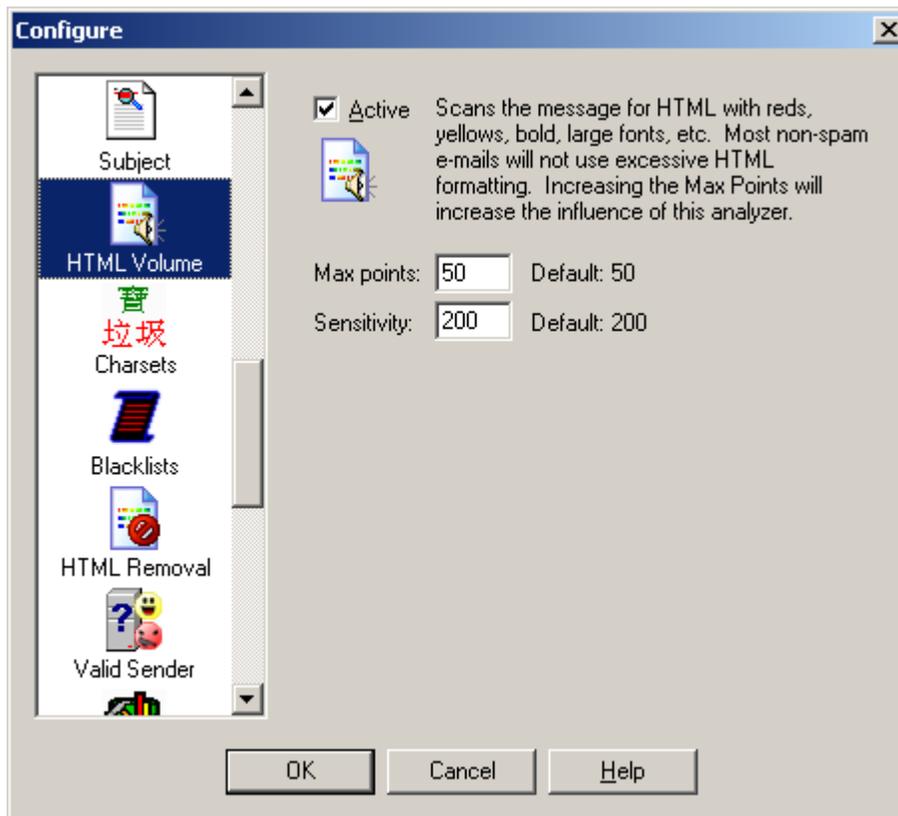
Points for empty subject - Set the points that will be assigned when a message has an empty or blank subject. This is common with spam, but may also occur when a friend sends you a message

and forgets to fill in the subject.

Use Defaults... - Sets Dictionary settings to the defaults.

3.2.12 HTML Volume

Do some of your e-mails just scream at you? The spammers want your attention. They use reds, yellows, bright blues, big fonts, embedded pictures, and other techniques not usually employed by your friends, relatives, and co-workers. The **HTML Volume Analyzer** looks for these elements in your e-mail and assigns points when it finds them. You can change how sensitive the **HTML Volume Analyzer** is, and the maximum number of points each e-mail message is allowed to contribute to the total.



The HTML Volume Analyzer looks at the "loudness" of the message. Most regular folks don't scream their message in bright reds and yellows in large fonts. Many spammers use these attention getting techniques. This analyzer assigns points for large fonts and bright colors.

You can control the maximum number of points that this analyzer contributes to the total report. If you feel it does a good job at distinguishing good e-mail from spam, you may want to increase the Max points.

If you have "loud" friends that e-mail you in big bold, red letters, then you may want to either turn this analyzer off, decrease its influence on the total score by lowering the Max points, or pick new friends.

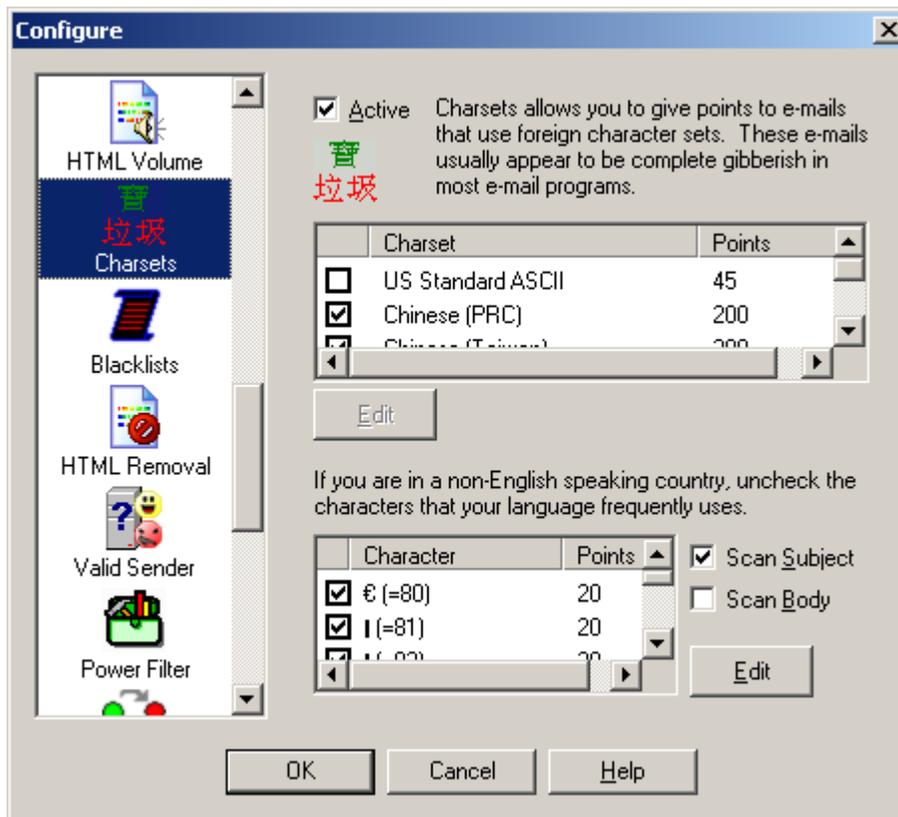
The sensitivity lets you set how "picky" this analyzer is. If you set it very high, it will give the max points for one large font. If you set it very low, then it will take lots of large **font** changes and

color changes to add points.

3.2.13 Charsets

Do you get e-mails where the subject looks like this -- ýÃûÔÚÂüÑÓ?

These are usually spam from China or Korea where they've specified a Chinese or Korean character set and your e-mail program won't display the characters. Spam Sleuth lets you detect and eliminate these e-mails with the **Charsets Analyzer**. By default the program will eliminate Chinese and Korean character sets.



The Charsets Analyzer lets you get rid of that annoying Chinese and Korean spam. Since most e-mail viewers don't show characters in the Chinese character set, these e-mails look like a string of gibberish like this - ÞÔýÔÚÂüÑÓ;ç°þ±±Ô»Ãû¹¼ÈË¾ÍÔâÑù.

Unless you read Chinese or Korean, we recommend that you leave the default characters sets checked. The Latin character sets are used by many regular e-mails, so we recommend that you leave it unchecked.

Spam Sleuth can also check for any high-bit characters. These are characters that are above the 127 in the ASCII set. All high-bit characters are selected by default. They are usually only used by non-English speaking countries. If you are in Germany, we recommend that you uncheck characters in your character set such as (Ä and ä). If you are in Mexico, we

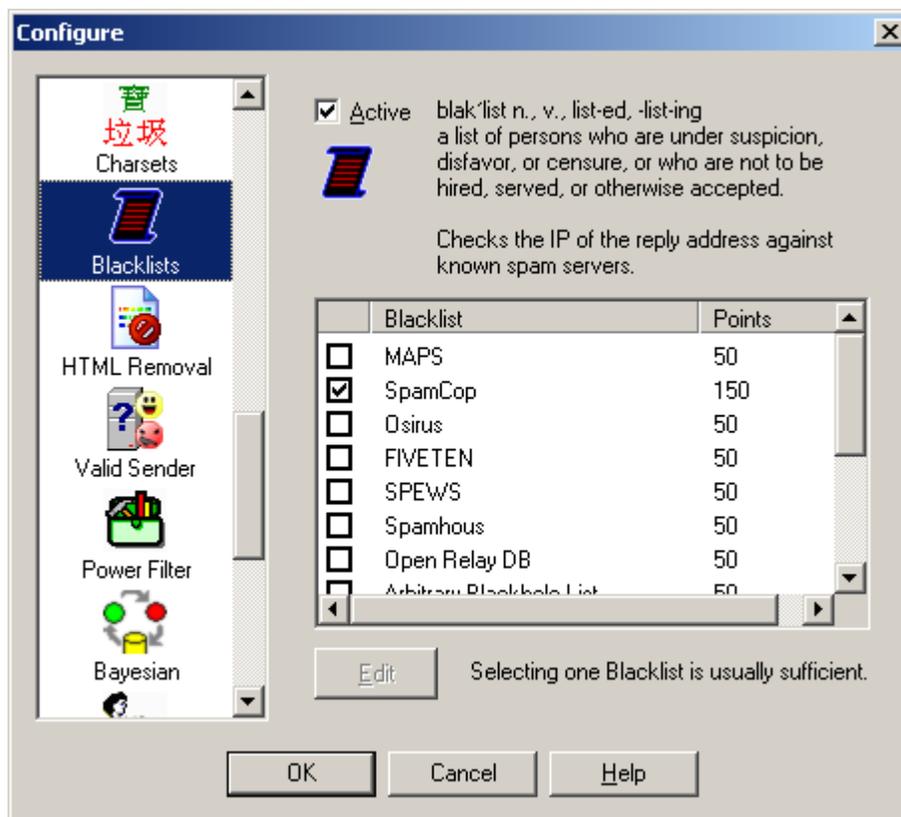
recommend that you uncheck your characters such as (Ã and ã). If your country uses other characters, we recommend that you uncheck them so that they aren't assigned points.

You can increase the points given for any particular character.

You can have Spam Sleuth scan the Subject of the message, and the Body of the message. By default, Spam Sleuth only checks the Subject.

3.2.14 BlackLists

Ever wish there was a comprehensive list of spammers? Well so do we, but unfortunately the closest thing is the blacklists. The blacklists contain the IP addresses of all the known spam servers and open relay servers (used by spammers). These lists of spam servers are built different ways. Some of them set spam traps where they put an e-mail address out on web pages and other public places so that it gets on the big lists of e-mails. Then they blacklist anybody who sends to that e-mail address. Others collect the spam e-mail from lots of people and if there are enough of the same message they assume it is spam and blacklist the server. The **Blacklist Analyzer** lets you check the list to see if the e-mail was sent from a blacklisted server. There are lots of blacklists and Spam Sleuth includes most of them. You should only use one at a time because they can take several seconds per message to check.



The BlackList Analyzer uses free blacklist databases to check whether the e-mail in question was sent by a known spam server. These databases allow Spam Sleuth™ to look up an IP address and determine whether it came from a known spam sending machine.

blak'list n., v., list-ed, -list-ing - a list of persons who are under suspicion, disfavor, or censure, or who are not to be hired, served, or otherwise accepted.

You may be tempted to turn on all of the black lists, but it really isn't necessary. Most of them contain the same or at least similar information. Some of them are subsets of the others. It would be better to increase the number of points assigned when the one blacklist reports that the e-mail was sent by a known spam server. By default, Spam Sleuth™ uses SpamCop, which seems to be one of the more accurate lists

These lists are built in different ways. Some of them use spam traps where they put a brand new e-mail address out on a web page and then "trap" everybody who sends to that e-mail. Some are built by taking a weighted average based on how many people send them copies of the same spam message from the same server.

Each list that you check will take 3 to 5 seconds to check if the e-mail is not from a spammer (negative response). It takes about 1 second to check if the e-mail is from a known spammer (positive response).

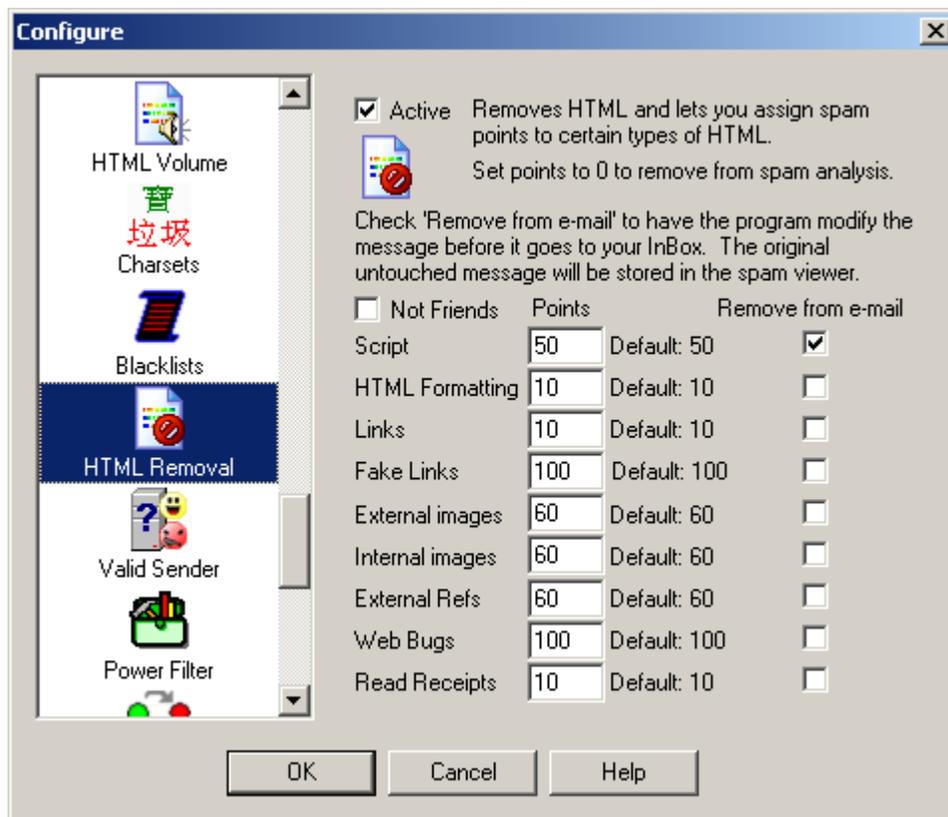
You can edit the number of points assigned when a blacklist reports that the IP is a known spammer.

3.2.15 HTML Removal

Are HTML e-mail messages dangerous? I guess it depends on how you define dangerous. HTML e-mail can run scripts, redirect to other web pages which may be pornographic, and even send information back to the sender that says you looked at the e-mail. The **HTML Removal Analyzer** is one of the more unique features of Spam Sleuth. It can selectively remove dangerous HTML from your e-mails. By removing script, you don't have to worry about being redirected to another web page. By default, Spam Sleuth will remove HTML script. You may lose some flying logos, but your computer will be safer. Some folks would prefer to get just the text without the colors, fonts, backgrounds, etc. If you just like the plain text without the frilly icing, then let the **HTML Removal Analyzer** take out the extraneous text formatting. The **HTML Removal Analyzer** can also remove links. Links are usually pretty safe because you have to click on them to go to a web page. For kids, however, you might consider removing links.

There are two kinds of images that can appear in an e-mail. There are embedded (internal) images, which use up your computer connection when the e-mail is sent, and the more dangerous kind – external images. The external images are stored on a web server. When the e-mail is viewed, your computer goes and gets the external images. Often times it also sends information to the spammer that you looked at the e-mail. This increases the chances of you getting more spam from that spammer in the future. If you choose to Remove images (External) in the **HTML Removal Analyzer** you will not see the pretty pictures in your spam or in your valid newsletters.

If you don't want spammers to know that you've read your e-mail, you may need to take out Web Bugs, External References and Read Receipt Requested header tags out of your e-mail. The **HTML Removal Analyzer** handles all of these.



The HTML Removal Analyzer is one of the most unique features in Spam Sleuth™. This analyzer can add points for certain types of HTML, but more impressive is its ability to remove certain types of HTML.

Script - Java Script and other scripting languages are programming languages, and have been known to have some security holes. Since many of the e-mail clients are using the browser, or browser component to read the e-mail, your computer may be put at risk just by reading an e-mail. Turning on Remove Script can remove the script (program) from the e-mail. Sometimes this means an ad doesn't "fly", but sometimes it means that a dangerous script virus has been thwarted.

HTML Formatting - HTML formatting in a message can be a good thing, but most of the time it is just used by the advertisers trying to get your attention. The meaning of the message is in the text, and conveying it in a big bright purple font isn't usually necessary.

Links - Most of the time links in a message are just fine. If you are using Spam Sleuth to protect kids, you may want to remove links that kids might click on and take them an unsavory web site. For most people, we recommend leaving this unchecked and keep the links. Beware, if you click on a link sent from an e-mail, there is a high probability that the web site owner now knows that you (as identified by your e-mail address) read their e-mail and followed their link.

Fake Links - Some e-mails are including links that are designed to deceive. The spammers

use special formatting to make it appear that you are going to your own bank or secure site, when really the browser is taking you to a dangerous site that will take your personal login information and use it to empty your account. An example:
`http://www.ebay.com_login@200.18.11.4/` While this looks at first glance to be going to eBay, it is going to a site residing at IP 200.18.11.4.

Remove Images (External) – We recommend leaving checking this option because most regular folks (friends, family, co-workers) do not send e-mail with external links. To do so requires that you have a web server, or hosting site, and that you are sending HTML with the intent that when the message is opened, the image will be loaded from the web server. Usually this is something that marketers do.

Remove Images (Internal) – This one isn't as bad as external images. The image has already been sent to you in the e-mail message. This is often used by spammers, but can easily be used by anyone who pastes a picture of themselves into an e-mail. Opening messages with just Internal images doesn't send anything back to the sender.

External Refs - Because HTML can reference other web pages, it is very likely that just viewing an HTML e-mail will cause your computer to request web pages. The clever spammers will track those requests and know that you've viewed their message. You can add points for external references, or eliminate them altogether by checking the checkbox for Remove from e-mail.

Web Bugs - Use of Web Bugs is a common practice among spammers. They will use IMG SRC tags in their e-mails which cause your computer to request an image when the e-mail is viewed. This wouldn't be so bad, except that now they tack your e-mail address onto the image request so that they know that you viewed their message. This seemingly safe image request will tag your e-mail in their database as live and you will get even more spam.

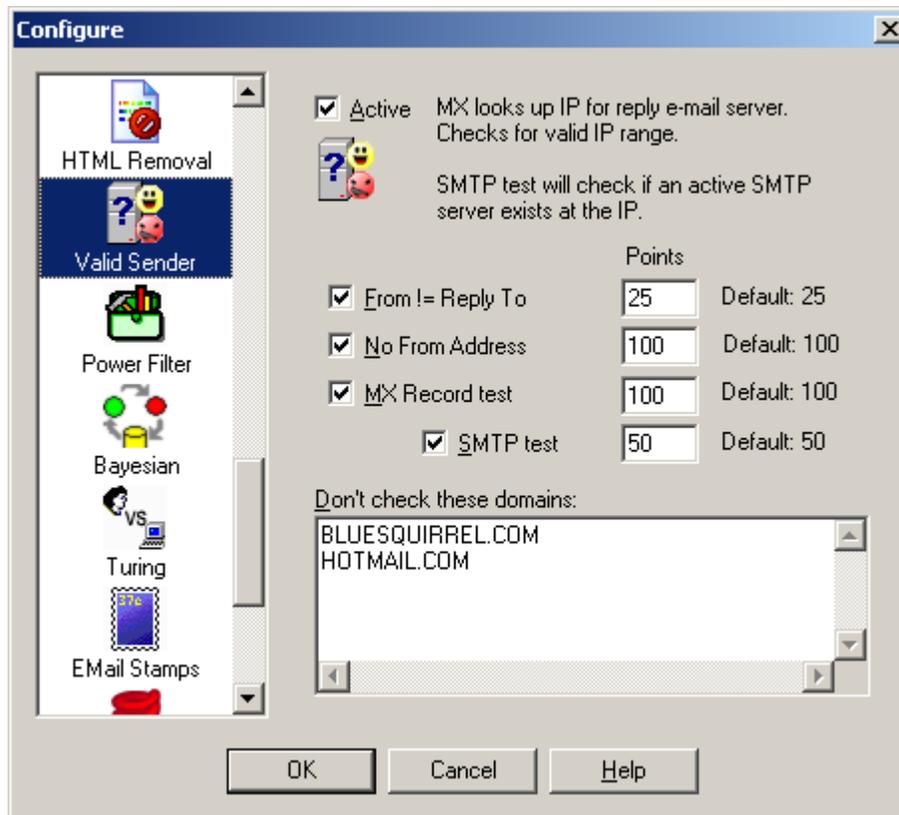
Read Receipts - This is an e-mail header tag that tells some e-mail clients to notify the sender that you've read their message. Some e-mail programs ignore it, some let you decide whether to notify the sender, and some just notify the sender automatically. Spammers don't use these very often, but you may want to remove the Read Receipt Request tags from your e-mail.

Assign points to these as you wish. Some valid newsletters use external images and some use internal images. If you don't subscribe to newsletters, you may want to increase the points.

3.2.16 Valid Sender

Have you ever wondered what would happen if you replied to spam and asked them to remove you from their list? If they aren't a reputable company (which many aren't) you will be flagged as a "live prospect" and your name will probably be sold to other spammers. By replying, you let them know that there is a real person at an active e-mail account. You may not be able to e-mail them back for a number of reasons. The **Valid Ssender Analyzer** looks for these reasons and increases the spam points if the e-mail fails the tests. If the "From" address is not the same as the "Reply To" address, it may indicate deception and some points will be added. The addresses not matching often occurs when a company hires a spam company. The "Reply To" goes back to the spam company so they can handle the backlash. The **Valid Ssender Analyzer** also looks for an empty

"From" address. If there isn't anybody to whom you can send a reply, it isn't likely that the e-mail is good. The final steps are to verify that there is an IP address to which a reply could be sent. If that works, then a quick test lets the **Valid Ssender Analyzer** know whether there is a real computer receiving e-mail on the other end.



The Valid Sender Analyzer looks at the sender of the e-mail to determine their willingness to accept a return e-mail. Usually spammers don't want to be contacted. They send out millions of e-mails and if even 1% replied to ask a question, it would be very bad for them.

The first test is whether the **From** is equal to the **Reply To** address. E-mails can have one address that specifies where it is from (often a lie), and another address for where a reply should go. If the two don't match it is a indication of spam. Sometimes a company (not very reputable) will contract with another company to handle the spam responses. In this case From might be joe@slimeycompany.com while the Reply To could be bucket@spam-handler.com.

The second test is whether there is a real e-mail address to which you could send a reply. The spammer might send no **From** address at all. If the **From** is blank, it probably means they don't want to be contacted and the probability is high that the message is spam.

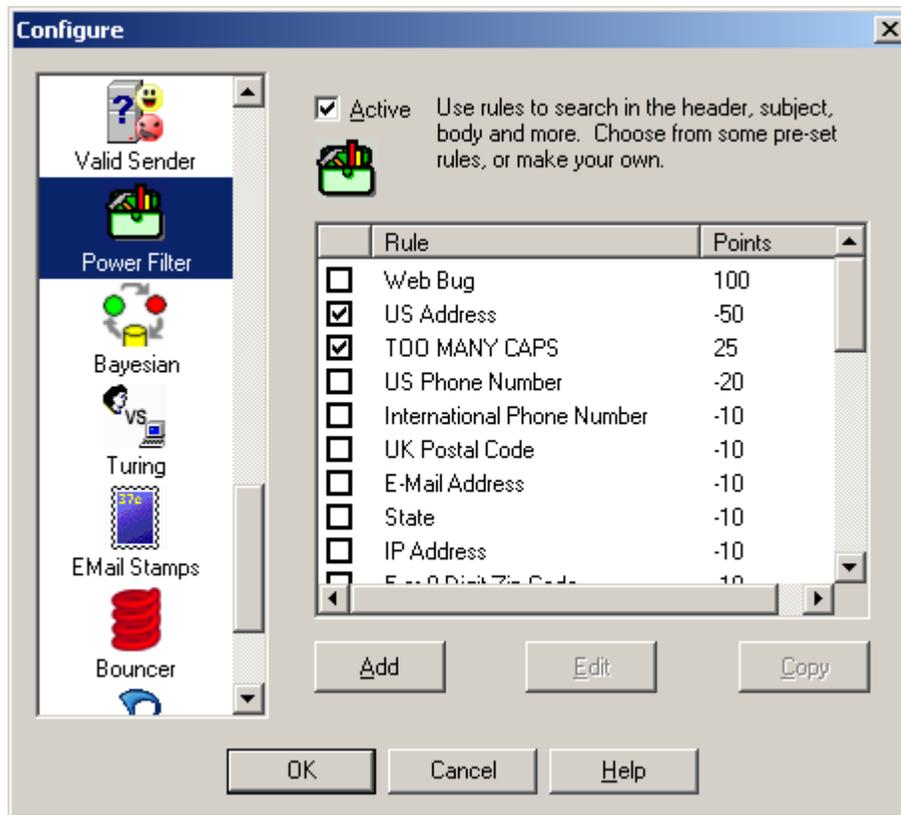
An MX Record test takes a few seconds. Your computer will look up the e-mail address and make sure there is an IP address available to send a reply if you wanted to send one. In the physical world this would be equivalent of looking up the return address on an envelope in the phone book.

If the MX Record succeeds then we can do one more test - the SMTP test. The SMTP test takes some time. We can check to see if there is a server there to accept our reply. In the physical world, this is equivalent of driving to the return address listed on the envelope and making sure there is a mailbox there.

You may not want to do an MX record check and SMTP test on every e-mail. Put those domains in the box. There are two good reasons not to do the test.

- 1) Some domains don't allow an SMTP test without first sending e-mail. These would fail the SMTP test every time.
- 2) Your business domain. There is no reason to check your own domain every time. At a company you would get lots of e-mail from that one domain.

3.2.17 Power Filter



The Power Filter Analyzer lets you set up very powerful filters that work on specific parts of messages. Set up filters that analyze just the Subject, or only the Headers.

Some pre-defined filters have been set up. You cannot edit the pre-defined filters. You can turn them on or off. If you want to change them, just make a copy, by selecting one and hitting the Copy button. Then you can turn off the pre-defined filter and tailor the copy to your own liking.

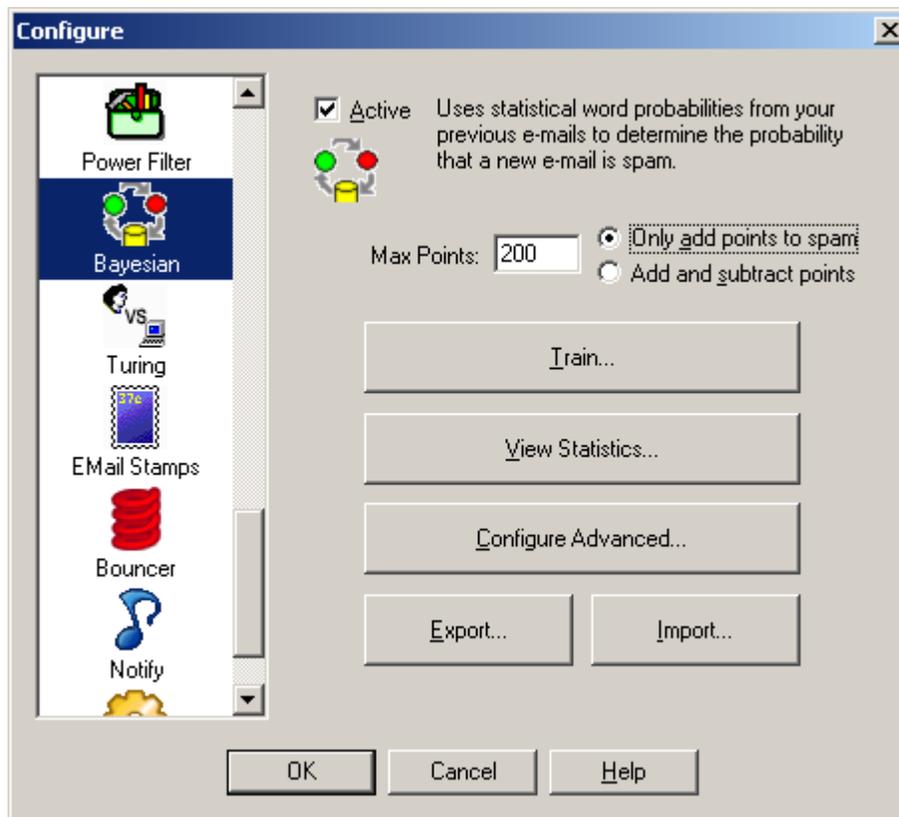
The pre-defined filters use a powerful regular expression syntax that allows complex pattern matching. The details of the regular expression syntax are listed in Appendix A. Be careful, as some complex regular expressions can take a long time to match in a large e-mail message.

3.2.18 Bayesian

What if there was a way that a computer could learn what spam looks like, then detect new and novel messages without being told about specific words or phrases?

The Bayesian Analyzer does this. It looks at your previous e-mail and learns the characteristics of

spam and good e-mail. Just like a baby, it needs to be taught right from wrong. By marking your messages as Good or Spam, and then Train the **Bayesian Analyzer**, you can teach it right from wrong. Then it can contribute to the decision of whether a new e-mail is spam or not.



The Bayesian Analyzer uses statistics to determine whether an e-mail is spam based on analysis of previous e-mails. We have included a brief description of how it works.

Max Points - sets the maximum number of points that the Bayesian Analyzer can contribute the spam score. If the Bayesian Analyzer is not certain, then only a couple of points might be added or deducted.

Only add points to spam - Setting this option will cause the Bayesian Analyzer to only add to the spam score. The number of points it adds is determined by the statistical analysis.

Add and subtract points - Setting this option will allow the Bayesian Analyzer to add points for spam and deduct points if the e-mail message is determined statistically to be a good message. With this option set, the Bayesian Analyzer can add or deduct Max Points.

You must train the Bayesian analyzer with previous e-mails. Training is not difficult, but it does require that you correct any mistakes that Spam Sleuth might have made in the past. You must also let Spam Sleuth keep your good e-mail so that it has both spam and good e-mail with which to train.

Steps:

1. Turn on 'Score and store non-spam messages'.
2. Correct any mistakes by using Mark as Good and Mark as Spam.
3. Hit the Train button

Train - Lets you train the analyzer with previous e-mails.

View Statistics - Lets you see how many e-mails have been trained and the distribution of probabilities.

Export... - Export the word probabilities to a comma separated (.CSV) file.

Import... - Import the word probabilities from a comma separated (.CSV) file.

3.2.18.1 How Bayesian Analysis Works

The Bayesian Analyzer uses Naive Bayesian statistics to calculate the probability that an unknown e-mail is spam or not. It uses the information from your previous e-mails to make its determination.

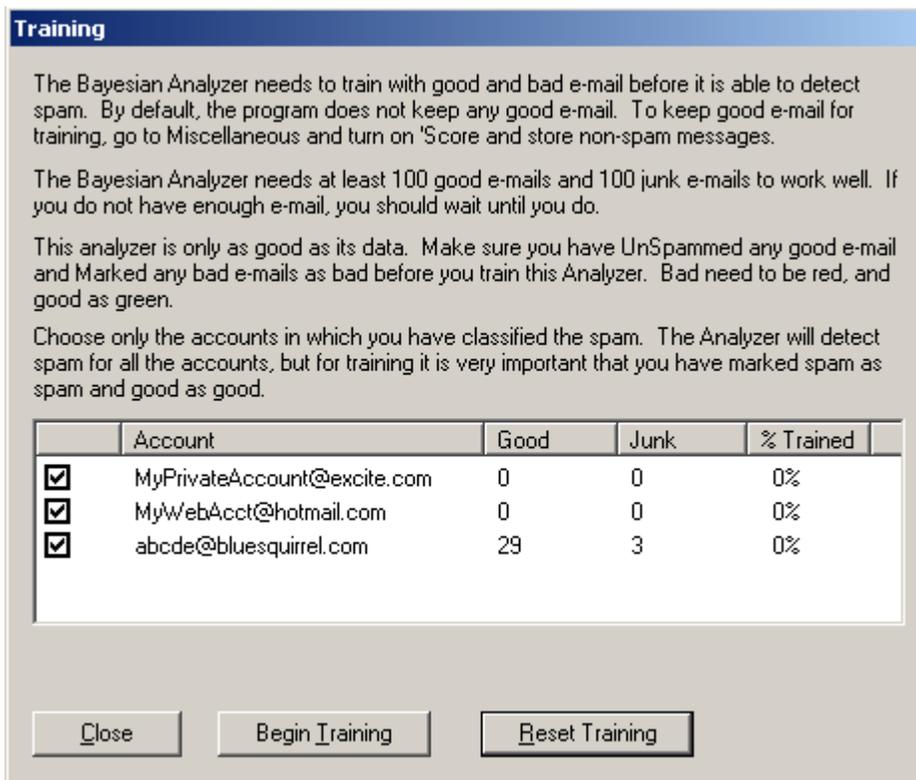
Every e-mail is broken down into words. For every word, the analyzer figures out the probability of a message being spam if that word appears in the text of the e-mail. This information is built during training. In order for the Bayesian Analyzer to figure out these probabilities, it must know in advance whether an e-mail is spam or good. Therefore, it is critical, that you correct any mistakes that Spam Sleuth may have made before training. If you don't correct the mistakes, the Bayesian Analysis will reinforce the mistakes.

Once the Bayesian Analyzer has figured out the probabilities for the words, it stores them in a dictionary file. If you want to see the word probabilities, you can Export the file in comma separated format.

When a new e-mail comes in, it is broken down into words, and the 15 most influential words are used to calculate a probability that the message is spam using formulas established by Thomas Bayes. The most influential words are those that have probabilities near 0 (absolutely a good e-mail) or near 1 (absolutely a spam e-mail). If you would like Spam Sleuth to use more or fewer words in its calculation, you can change it in the Advanced settings.

The end result from the Bayesian Analyzer is a probability that the e-mail is spam. This is converted into points using an logarithmic algorithm which adds or subtracts many points when the Bayesian Analyzer is certain of its decision. The Bayesian Analyzer adds or subtracts only a few points, or none at all, when it is not very sure whether an e-mail is good or spam.

3.2.18.2 Train



To train the Bayesian analyzer, you should have good e-mail, and spam e-mail. You should have at least 100 of each. If you do not have 100 of each, we recommend that you wait until you do.

If you do not have any good mail, then make sure you have turned on 'Score and store non-spam messages'

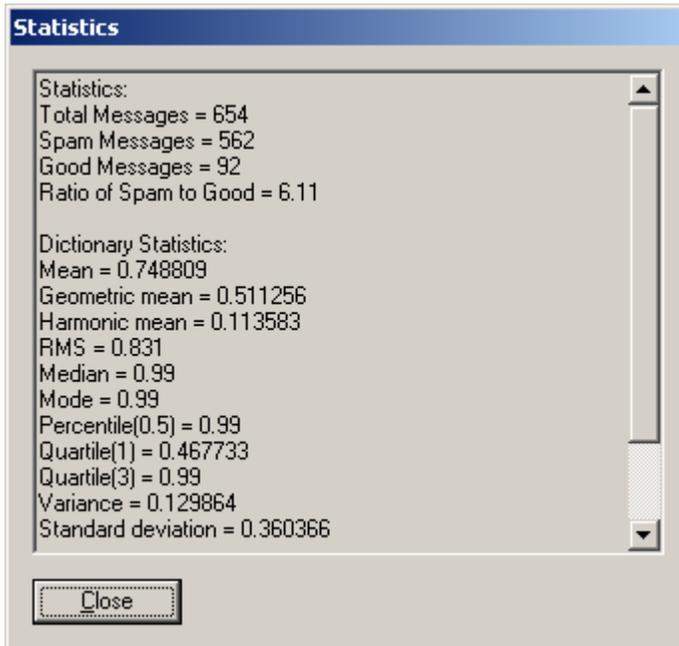
Choose only the accounts for which you have categorized the e-mail as spam and good. The spam messages should have a red dot next to them, and the good messages should have a green dot next to them. Spam Sleuth will do most of the work automatically, but you need to correct any mistakes it may have made before training.

Begin Training starts the training. If you have trained on some e-mails already, then any new e-mails will be added to the dictionary.

Reset Training will erase all the training. We recommend you do this if you have bad training.

The **% Trained** will always show 0% when you enter. The % trained will change as it trains.

3.2.18.3 View Statistics



This shows the statistics for the Bayesian Analyzer. If you have not trained the Bayesian Analyzer, you must train it first.

3.2.18.4 Advanced



This lets you set some advanced features and settings of the Bayesian Analyzer.

Significant Words - By default, the Bayesian Analyzer uses the 15 most significant words (by their probability) to determine whether the e-mail is spam or good.

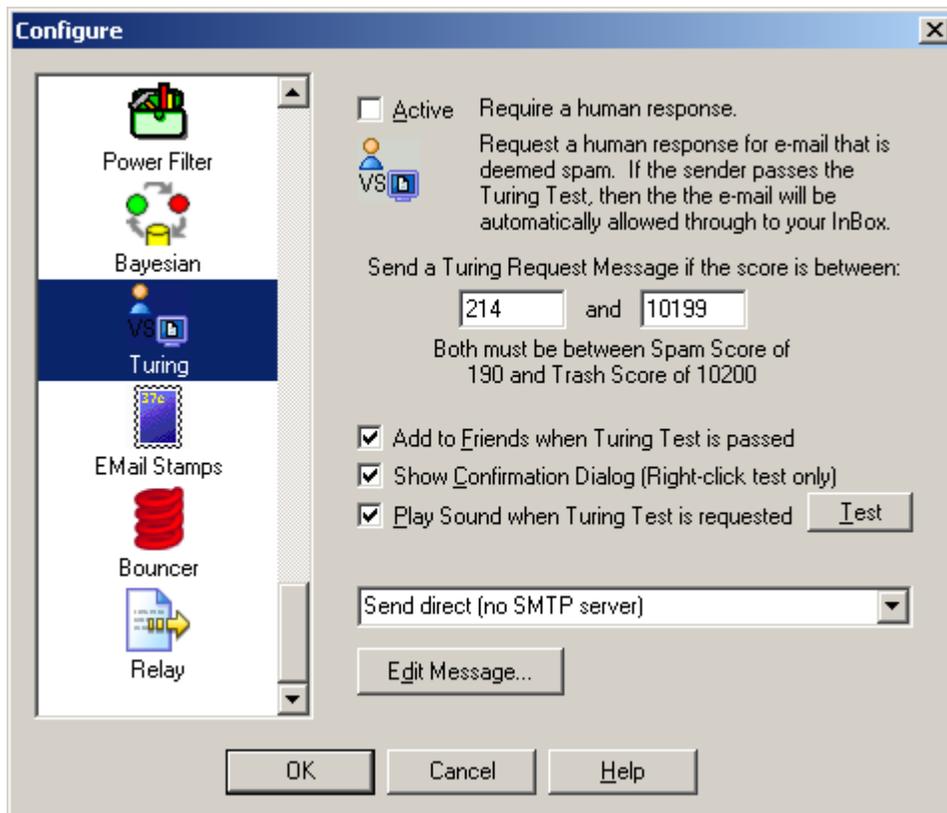
Prune dictionary after training - determines whether the dictionary will be purged of non-significant words before saving. The non-significant words are words that have not appeared enough times in your spam or good e-mails to be considered in the calculations. This is not selected by default because if you train incrementally, the word counts need to be retained because one additional e-mail might cause the word to be significant. If you Prune the dictionary after training, the dictionary file will be smaller, but the word counts for non-significant words will not be retained for future training sessions.

3.2.19 Turing

What if there were a way to **make sure** you get good e-mail even if Spam Sleuth detected it as spam for some reason?

Well there is, but you have to turn it on. We **highly recommend** that you turn this Analyzer on. The only reason it isn't on by default is that it sends out e-mail.

The Turing Analyzer will send a challenge e-mail message to any message detected as spam, and give them a chance to take a test to let their message through. The spammers won't do it, but everyone else will.



The Turing Test is a great way to make sure you get important e-mails, but still screen out the automated spam. It is not on by default, but we recommend that you turn it on.

The default is to send a Turing Test for all messages between the Spam Score and the Trash Score. You can choose a different range if you'd like.

If an e-mail is determined to be spam, you can request a Turing Test. This request will send an e-mail back to the sender requesting that they prove they are human, and not an automated spam machine. There will be a link in the e-mail that takes them to a web site where they can pass an easy (for humans) test, then the original e-mail they sent will be marked as good, and released to your InBox.

Add to Friends - Selecting this option will add everyone who passes the Turing Test to your Friends list so their future e-mails will be automatically accepted.

Show Confirmation Dialog - Decide whether to show a confirmation when using right-click to request a Turing Test.

Play Sound when Turing Test Requested - Plays a sound when requesting a Turing Test (automatically or with right-click). To change the sound, replace the `TuringReq.wav` file in the program directory.

This is a really great Analyzer to turn on if you want to make sure you get e-mails from long lost friends and people who are trying to reach you.

Edit Message... - Allows you to edit the Turing message.

The message will be available (to be released by the Turing Test) for the same number of days that you keep your spam. The default is 30 days, but you can increase or decrease it by going to the Score settings.

Important Note: You should turn on *Turing Test* or *EMail Stamps*, or *Bouncer*, but you should only turn on one of them.

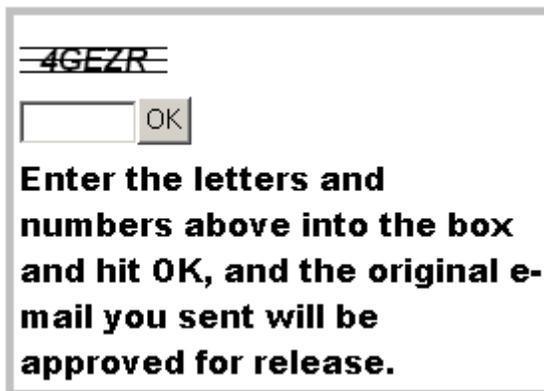
Advanced Capabilities

- **Trigger Message Absorption** - Deletes the message that triggers the release of an e-mail so the entire process is transparent to you.
- **Bounce Absorption** - Hides Turing Requests that bounce back because the spammer faked their e-mail address.
- **E-Mail Loop Detection** - Won't send another Turing Request to the same e-mail address within an hour to avoid rapid sending back and forth with a vacation auto-responder.

3.2.19.1 Turing Test

The Turing Test is named after Alan Turing. Alan proposed a test in the 1950's to distinguish a human from a machine.

The Turing Test used by Spam Sleuth is a simple test which is not easily automated by a computer. The test taker simply enters the letters shown into a box. The letters are partially obscured to make it more difficult for a computer to pass the test.



When a Turing Test is requested, an e-mail will be sent back to the sender, which requests that they click on a link and verify that they are human. Once they've passed this simple test, a message will be sent to your e-mail box which releases the original e-mail to your InBox.

The net effect is that you can set your spam screening even tighter (lower your spam threshold score) with assurance that if a good message is mistaken for spam, the original sender will get a chance to prove they are not a bulk spammer and their message will be delivered.

3.2.19.2 Sample Turing Message

I use Spam Sleuth to screen all my e-mail. The message you sent to me has been queued for delivery, but has not been delivered because Spam Sleuth did not recognize your From address.

If you would perform the following simple action, your message will be delivered to my InBox and your From address will be added to Spam Sleuth so that any further e-mails from you will go straight to my InBox for my prompt attention.

Go to:

<http://www.spamsleuth.com/t/t.html?T=ASampleAYmx1ZXXndWlycmVsLmNvbSx0cm9uYmxhMessageob28uY29tLDAzMDUwTjEyMTgxNjczMg==>

At that site, you will be asked to type a few letters. The e-mail you sent earlier will then be automatically delivered to my InBox. You won't need to send your message again.

3.2.19.3 Advanced

The Turing Analyzer gets e-mail messages that release the e-mail messages when senders pass the Turing Test. These messages are deleted unless you change this setting.

TURING.INI

[Settings]

RemoveTuringNotifications=1 ;Default is 1 - Set to 0 to keep those messages

The Turing Analyzer sends e-mail requests which may bounce if the e-mail address has been faked or is no longer valid. The Turing Analyzer can absorb those bounces so that you don't see them. To turn off this feature, set the value to 0.

RemoveTuringRequestBounces=1 ;Default is 1 - Set to 0 to keep the bounces

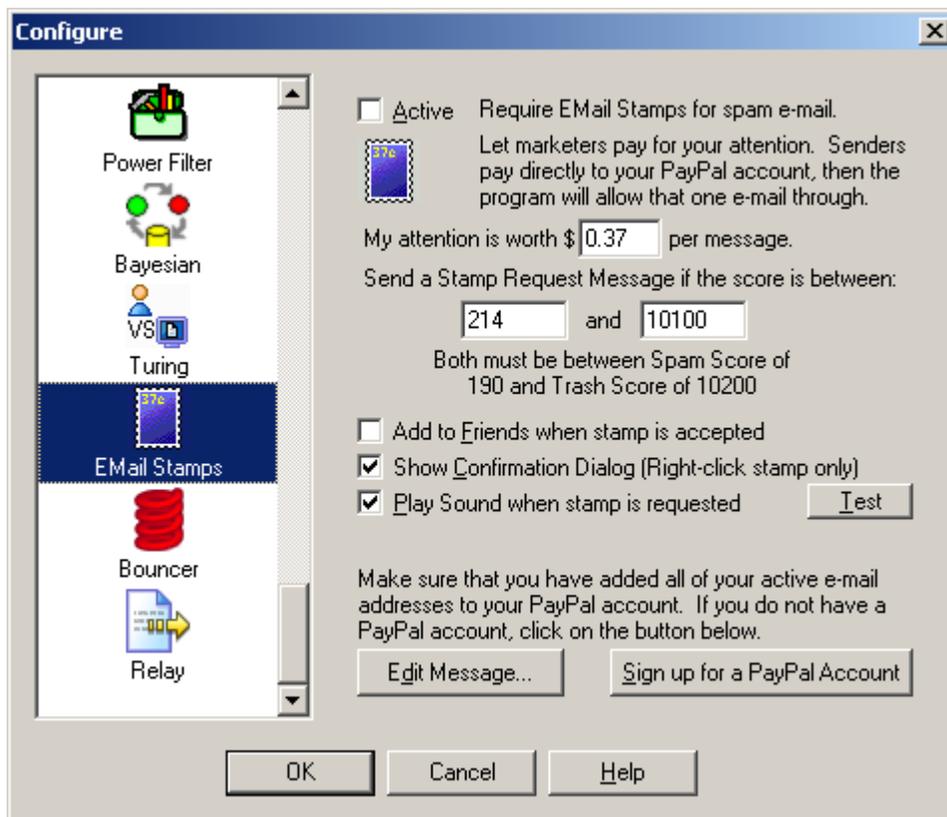
3.2.20 EMail Stamps

Have you ever said "If I had a nickel for every spam I get..." Well, now its possible.

Just turn on **EMail Stamps**, and spammers will get a request for a nickel. If they pay the nickel, you keep the nickel, and the e-mail is allowed.

If your time is worth more than a nickel a message, just change it to a dollar, or more.

We recommend turning on Turing or **EMail Stamps**, but not both.



The EMail Stamps Analyzer is not active by default.

The EMail Stamps Analyzer will automatically request a payment from an unknown sender. When an e-mail reaches a certain points threshold, it will ask for an EMail Stamp. The sender (probably a spammer), will receive an e-mail requesting a payment be made to allow their e-mail to be released to your InBox.

The request e-mail is not sent unless the message reaches the points threshold that you set. Anyone listed in Friends or Mailing Lists will not get the EMail Stamp request. Most messages that do not have junk characteristics will not trigger the request (unless you set the custom points very, very low).

You set the amount requested. It can range from a penny (\$0.01) to almost a thousand dollars (\$999.99). Do not expect to get rich from this. Most spammers do not look at the responses to their blast e-mails. Thirty-seven cents (\$0.37) is a reasonable amount. A long lost friend might pay it to get in touch with you, and you can give the money back when you go to lunch.

Spam Sleuth queues the e-mail and if/when payment is made, the e-mail is released to your InBox.

To use this Analyzer, you will need an active PayPal account. You can click on the "Sign up for a PayPal Account" if you don't already have one. It is free to sign up, but you do provide a credit card or bank account. PayPal is an independent third-party payment processor. The PayPal sign up link does send our affiliate ID to PayPal as a referrer.

For this Analyzer to work properly, your PayPal account must be linked to your e-mail address. A PayPal account can have up to seven e-mail addresses.

Edit Message... - Allows you to edit the EMail Stamp outgoing message.

If you **want** to read the message before the sender/spammer pays you, you can. The message will be in the Mail Jail marked as spam.

Click [here](#) to go online and see a sample EMail Stamp request.

Important Note: You should turn on *Turing Test* **or** *EMail Stamps*, **or** *Bouncer*, but you should only turn on one of them.

Warning: The EMail Stamp request sent to the sender/spammer will identify your PayPal account by e-mail which is linked with your name. If you are uncomfortable with this, then do not activate the EMail Stamps Analyzer.

3.2.20.1 Sample EMail Stamp Request

Subject: EMail Stamp Request for {The Original Subject}

I use EMail Stamps to curb the flow of unwanted junk e-mail. Your message has been queued for delivery. If you would like your message delivered to my InBox, it will cost you \$0.37.

This modest sum is enough to keep unwanted junk e-mail from flooding my account. This e-mail was sent to you only because you contacted me by e-mail. Thank you for your understanding.

If you choose not to pay, I completely understand, and I respect your decision.

If your message is important, and you choose to pay \$0.37 to allow your e-mail through, the message will be automatically sent once PayPal informs me that the payment has been made. There is no need to send the message again.

You can pay me securely by PayPal with Visa, Mastercard, Discover or American Express. If you do not have a PayPal account, you can sign up for one at no cost.

Pay through PayPal

[Sign up for PayPal](#)

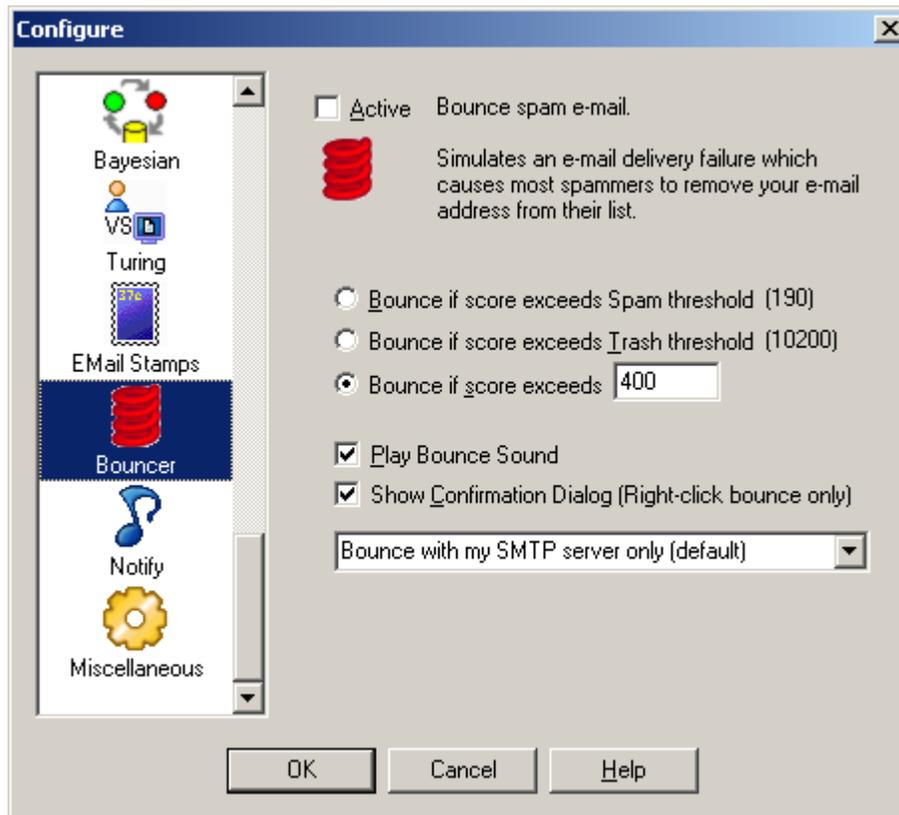
3.2.21 Bouncer

Ever wish you could just automatically get off the spammers lists? Well the only way they'll take you off their lists is if you don't exist. The **Bouncer Analyzer** can do just that. Or, at least make the spammers think you don't exist.

When the spammers send an e-mail to a non-existent account, they get a non-deliverable e-mail back from the last e-mail server in the chain. The **Bouncer Analyzer** can fake that non-deliverable e-mail and send it back to the spammers making them think you have dropped off the planet. They take you off their list and everybody wins (except the spammer).

If you want to make sure you get important messages, we recommend that you turn on Turing

instead.



The Bouncer Analyzer is not active by default.

The Bouncer Analyzer will look at the Total Score for the message and if it exceeds the specified threshold, it will simulate an e-mail bounce. An e-mail bounce is a message usually sent by an e-mail server to let the sender know that their message was not deliverable. The simulated bounce will let the spammer know that your e-mail address doesn't exist anymore. This will cause most of the junk e-mailers to remove you from their list. They don't want to spend their resources sending e-mail to non-existent accounts.

Using this will cut down on the amount of spam that you receive in the future.

It is turned off by default because it sends out e-mail.

Bounce Method:

Bounce with my SMTP server only (default) - Uses the SMTP server you have set for the account to send a non-deliverable report (bounce).

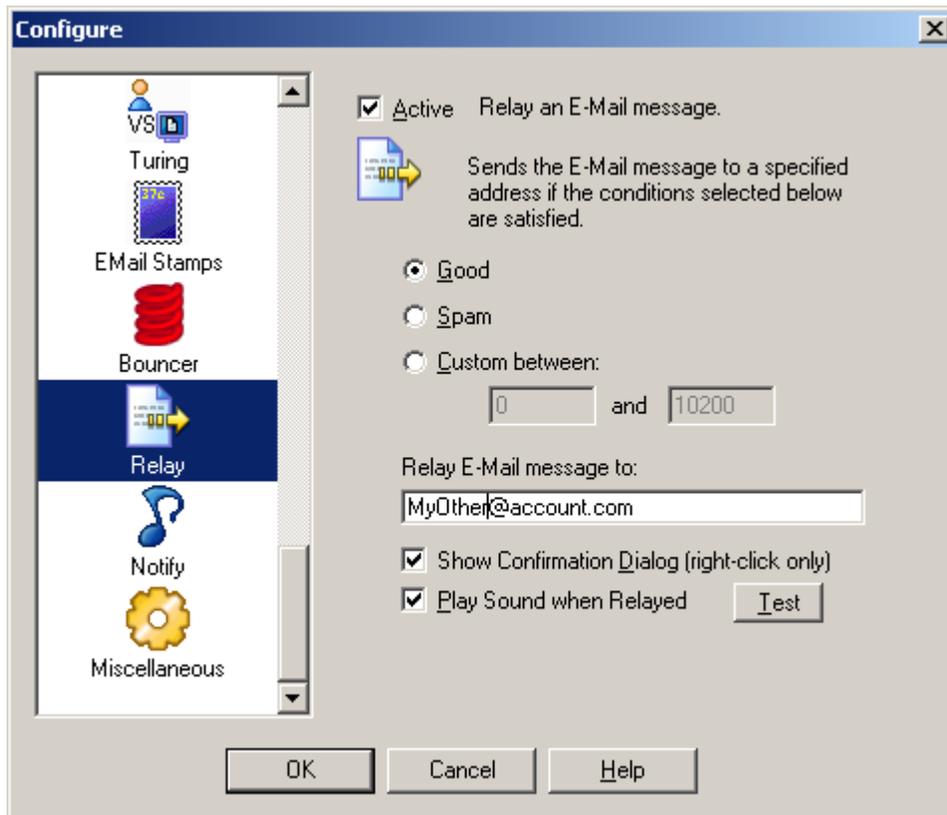
Bounce direct only - Sends the non-deliverable report (bounce) directly to the SMTP server of the sender. This will usually be slower. Choose this one if the default gives you a message every time that the bounce failed.

Bounce with my SMTP server then direct - Tries to send using your SMTP server which may fail be rejected (depends on your SMTP server), and then it sends direct.

Important Note: You should turn on *Turing Test* or *E-Mail Stamps*, or *Bouncer*, but you should only turn on one of them.

3.2.22 Relay

Do you want to screen e-mails on a junk account and forward the good stuff to your "real" e-mail account? Or, do you have an e-mail account on your cell phone or PDA that you only want the really good e-mail from Friends, your boss, etc. Use the Relay Analyzer to automatically forward the best e-mail.



The Relay Analyzer can relay messages based on its score. It is not on by default. This is useful for sending important messages to a PDA account, a pager, etc. You can protect your PDA e-mail account by giving out your regular e-mail address and then only passing along e-mail that is from a known Friend.

Good - Only relay messages that don't reach your spam threshold.

Spam - Only relay messages that exceed your spam threshold.

Custom - Set a custom score range. Perhaps you only want to relay messages that are from Friends, set the score to -20000 to -20000

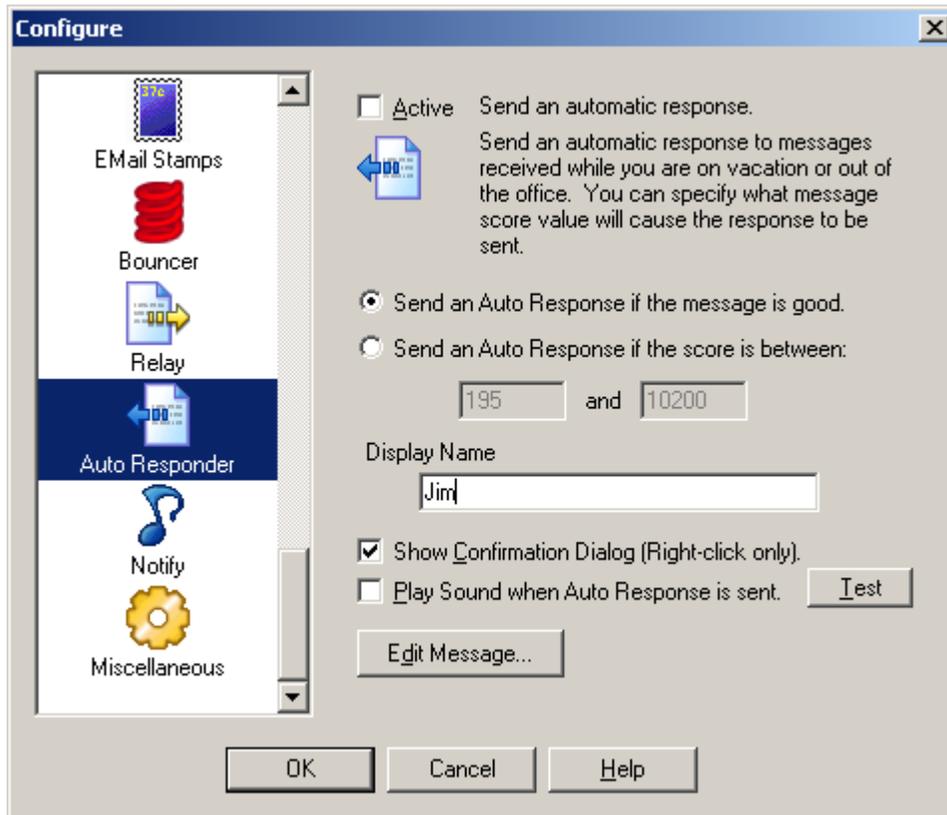
Relay E-mail message to: - Set the e-mail address of a valid e-mail account.

Show confirmation dialog (right-click only) - Check this option if you want to see a confirmation dialog when messages are relayed.

Play sound when Relayed - Check this option if you want to play a sound when messages are relayed.

3.2.23 Auto Responder

Are there times when you can't respond to your e-mail? Use the **Auto Responder** to let people know that you are away from e-mail, but you'll get back to them when you are able. Perhaps you've changed your address and you'd like to automatically let people know to use a different e-mail address in the future.

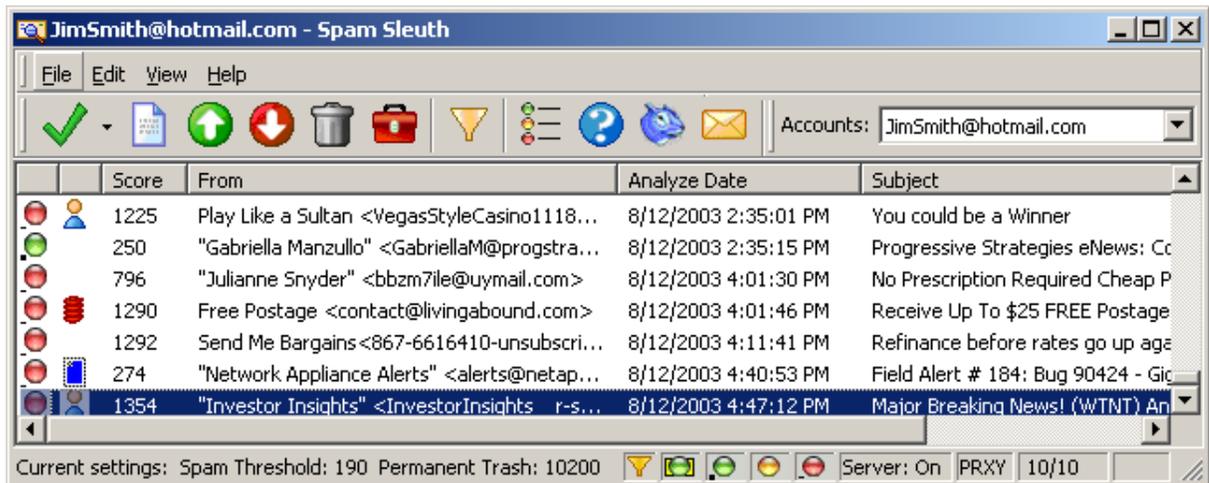


The Auto Responder sends an automatic message. A default message is included, but you can edit it to say whatever you'd like. The message will go back to the sender as listed in the From: or Reply To:.

This Analyzer is not on by default. You should only turn it on if you want an automatic reply.

The **Auto Responder** does influence whether the message reaches your InBox.

3.3 Mail Jail



The Mail Jail stores the spam for a short period of time.

Here are the reasons you would store spam:

- To provide a way to get a good message back if the program incorrectly determines it to be spam.
- To provide a set of spam so the Bayesian Analyzer can train.
- To be able to see reports on how and why a messages was marked as spam.
- To provide a list of spam mail so you determine the effectiveness of the program.

The Mail Jail also provides these abilities:

- To view spam messages in a safe environment.
- To keep a report for every spam.
- To recover a message that was marked as spam.
- To keep a report for every non-spam if you choose "Score and store non-spam messages"
- To see spam for a single account or for multiple accounts in one place.
- To select and request Turing.
- To select and bounce messages.
- To select and request EMail Stamps.
- To add sender's addresses to Friends.
- To add spammer's addresses to Spammers.
- To rescore messages to assist in tuning.
- To see the results of a Bayesian test for previous messages after training.
- To see amount of spam that you receive on a daily basis.
- To view spam reports for messages.

The Mail Jail lets you view your spam. It lists the score, who it was from, an action status, the date (as reported by the e-mail message) and the subject. You can double-click to view a message in a safe viewer. The viewer will not show pictures, it will not run Java script, and it will not let you launch an attachment.

 There is a red dot next to spam messages that were analyzed and found to be spam. These messages will always contain the unmodified message. The report may specify that the HTML or Attachments were removed, but if you Mark as Good (UnSpam) these messages, you will get the message as originally sent.

 There is a yellow dot next to messages that are stored for your convenience because the original message was modified before being sent to your InBox. The message might be modified to remove a dangerous attachment, or potentially harmful script. Any time the original message is modified, a copy of the original is stored. If you want the original (untouched) message, just click on message and hit  "Mark as Good (UnSpam)"

 There is a green dot next to messages that were not spam. You will not see any green dots unless you turn on the Score and Store non-spam messages in the Misc. section of configure.

The Spam Score column shows you how many points the e-mail received. Be aware that it may not be the total score, because there is a Stop Score that lets Spam Sleuth stop analyzing a message. If you always want a full report set the Stop Score to 0 in the Score configuration.

Sort the columns by clicking on a column header. Click it again to sort either ascending or descending.

Each e-mail account gets its own spam storage. Choose which account to view with the drop-down box of accounts in the upper right-hand corner. This is only available if you turn on AllowUserToggle.

You can *right-click* on an e-mail message and choose from the available options:



- Deletes the highlighted message(s).



- Displays the current message and spam report.



- Mark as Good (UnSpam) – Sends the message back to your e-mail program.



- Mark as Spam - sets to a spam message and keeps it from being delivered to your InBox.



- Displays the Program help.



- Turns the Filter on and off.



- Displays the legend for the color coded dots that appear next to the messages.



- Automatically opens your Web browser and launches the Blue Squirrel home page.



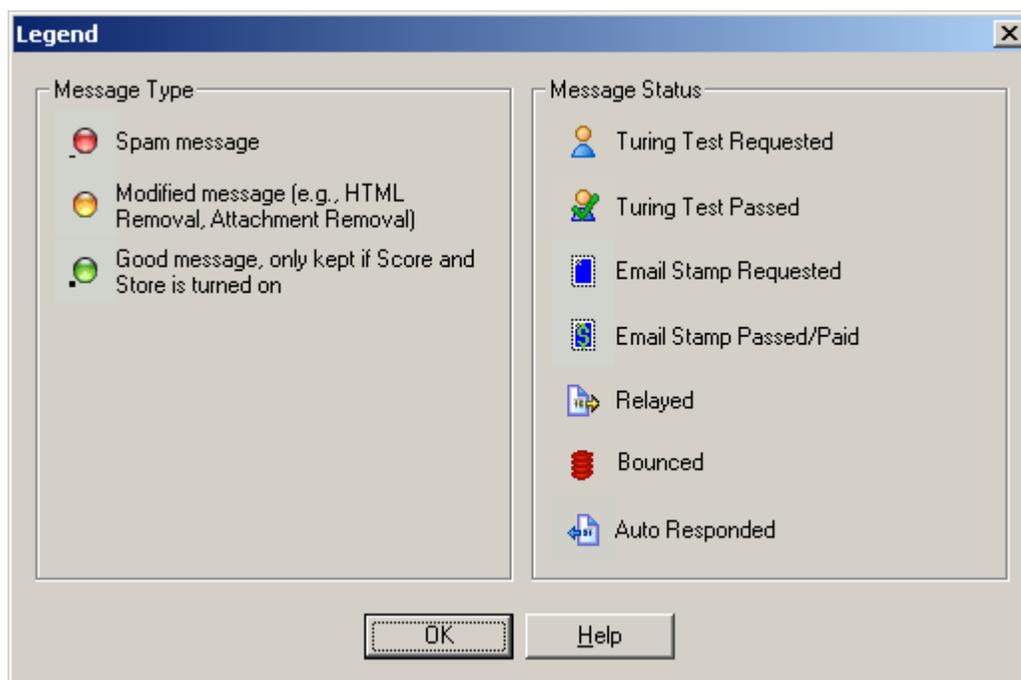
- Launches the Configuration dialog box.

When you double-click on a message, or choose the  icon, the message will be displayed in a safe message viewer. The message viewer will not format HTML, will not run Script, and will not decode attachments. It shows you the raw message that was sent. This is sometimes very helpful to see, as you can see the tricks that spammers use to hide their message from simple filters.

3.3.1 Drag and Drop

You can 'Drag and Drop' individual messages from Outlook or Outlook Express into the Mail Jail to "Add to Friends" or "Add to Spammers". The Mail Jail must be visible and the message must have a valid From: address.

3.3.2 Legend for Spam Message Types



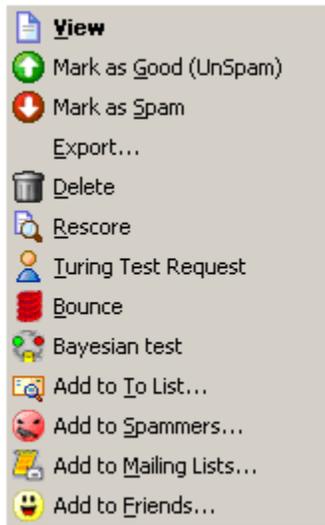
Spam message - This indicates an e-mail message was assigned points by the analyzers and the total points exceeded the spam threshold.

Modified message - This indicates an e-mail message that was modified by one or more of the Analyzers when it was being analyzed. The modified message was sent to your InBox. The original message is being held in the Mail Jail. If you need the original message, you can right-click on it and choose UnSpam.

Good message - This indicates an e-mail message that was assigned points by the analyzers and the total points did not reach the spam threshold.

It is important to note that the Good message and Spam message status is set at the time the message was analyzed, and does not change automatically when you change your spam threshold score.

3.3.3 Right Click Menu



View - Lets you view the message in the safe viewer.

Mark as Good (UnSpam) – Sends the e-mail back to your e-mail program. The message is re-mailed to your internal server.

Mark as Spam - You only need to use this if you intend to use the Bayesian Analyser. This option lets you categorize e-mail as spam.

Export – Saves a copy of the message (uncompressed) to a directory.

Delete – Deletes the message (will confirm if you have deletion confirmation turned on). Messages will be sent to the Recycle Bin unless you hold down SHIFT.

Rescore - Lets you re-score a message. This can be used for tuning. Scores may not be identical because some meta-information is not available on rescore.

Turing Test Request - Only available if the Turing Analyzer is active.

Bounce - Bounces an e-mail - See the Bouncer Analyzer for more information.

Bayesian Test - Shows you the score that the Bayesian Analyzer would give the message.

Add to To List – Adds the e-mail address in the "To:" section of the e-mail to the list of acceptable addresses. If you accept e-mail to several different e-mail addresses in the same account, you should add every one to the To Analyzer.

Add to Spammers – This will add the sender's e-mail address to the list of Spammers so you don't get a message from them again.

Add to Mailing Lists - This will add the To: field of the e-mail to the Mailing List. Use this when the From: field is always different, but the messages are sent to a list such as wine_enthusiasts@mailserv.net.

Add to Friends – This will add the sender's e-mail address to the list of Friends so you always get their e-mail in the future.

3.3.4 Menu

3.3.4.1 File

3.3.4.1.1 Configure...

Takes you to the Spam Sleuth configuration, where you can configure the Accounts and Analyzers.

3.3.4.1.2 Export...

Exports a message from its compressed format to a .MSG file which can be read by a text viewer.

3.3.4.1.3 Exit

Exits the program. This is different than hitting the X icon in the upper right-hand corner. The File->Exit will close the program completely.

3.3.4.2 Edit

3.3.4.2.1 Delete

Deletes the selected message(s) permanently and removes them from the Mail Jail. Deleting messages moves them to your Recycle Bin, so they can be recovered until you empty your Trash. If you don't want messages moved to the Recycle Bin, hold down SHIFT when you delete.

3.3.4.2.2 Delete All

Deletes all the messages from the Mail Jail after confirmation. Deleting messages moves them to your Recycle Bin, so they can be recovered until you empty your Trash. If you don't want messages moved to the Recycle Bin, hold down SHIFT when you delete.

3.3.4.2.3 Mark as Good (UnSpam)

Delivers the message to your InBox.

Sends the e-mail back to your e-mail program. The message is re-mailed to your internal server.

3.3.4.2.4 Mark as Spam

Marks the message as spam and turns the icon red. This is important for the Bayesian Analyzer for proper training.

3.3.4.2.5 Select All

Selects all the messages in the Mail Jail.

3.3.4.2.6 Refresh

Reloads the list of spam from the server. In most cases this is automatic.

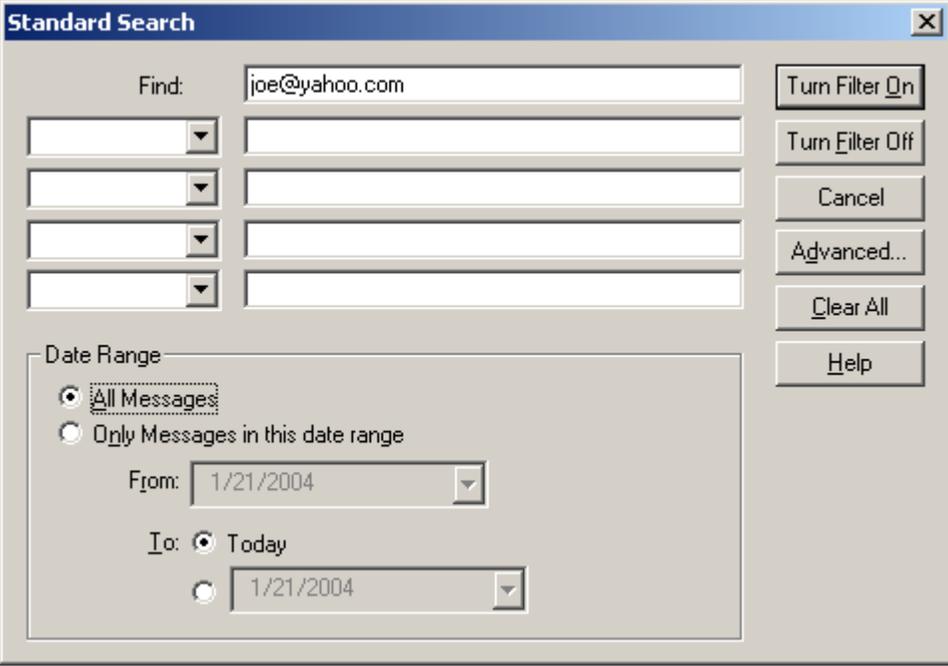
If you are running the server on an NT 4.0 server, or have turned off the service which notifies clients of file changes, the refresh will not be automatic.

3.3.4.2.7 Filter...

This menu option turns the filter on or off. The filter indexes your messages and lets you find a message that Spam Sleuth might have missed, or that you were expecting.

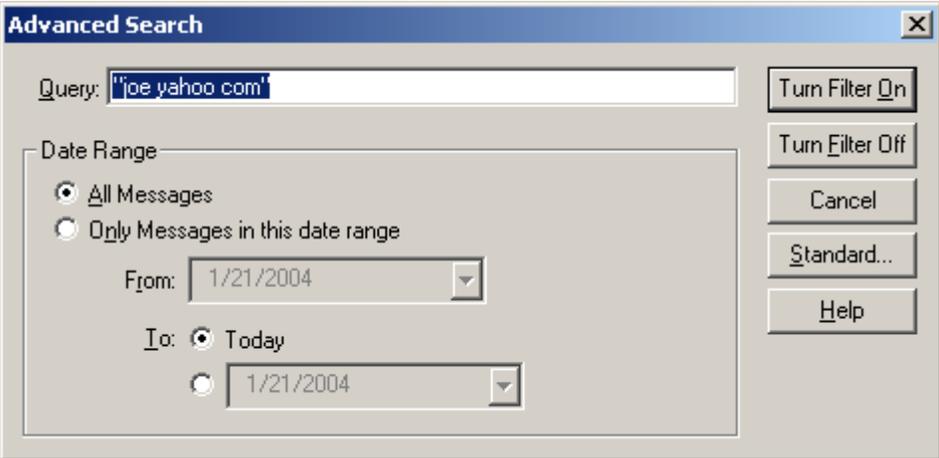
Each time you use the filter, the program will index the messages that have not yet been indexed. If the index is too out-of-date, the entire set of messages will be re-indexed.

Tip: If you leave the filter on, and the Find: fields are blank, you will see all of your messages, but the messages will be indexed as they come in. This is useful if you use the Filter feature often and would like to keep the index current.



The Standard Search dialog box features a title bar with a close button. It contains a 'Find:' label followed by a text input field containing 'joe@yahoo.com'. Below this are four rows, each consisting of a dropdown menu and a text input field. To the right of these fields are five buttons: 'Turn Filter On', 'Turn Filter Off', 'Cancel', 'Advanced...', and 'Clear All'. At the bottom right is a 'Help' button. A 'Date Range' section is located below the main search fields, containing two radio buttons: 'All Messages' (selected) and 'Only Messages in this date range'. Below the radio buttons are two date selection fields: 'From:' with a dropdown menu showing '1/21/2004', and 'To:' with a radio button selected for 'Today' and a dropdown menu showing '1/21/2004'.

If you want more control over the searching, you can use the Advanced Filter which gives you more control, but you need to use the syntax of the search language. See Appendix B for more information on the Advanced Filter Syntax.



The Advanced Search dialog box has a title bar with a close button. It features a 'Query:' label followed by a text input field containing '"joe yahoo com"'. Below this is a 'Date Range' section with two radio buttons: 'All Messages' (selected) and 'Only Messages in this date range'. Below the radio buttons are two date selection fields: 'From:' with a dropdown menu showing '1/21/2004', and 'To:' with a radio button selected for 'Today' and a dropdown menu showing '1/21/2004'. To the right of the main search fields are five buttons: 'Turn Filter On', 'Turn Filter Off', 'Cancel', 'Standard...', and 'Help'.

3.3.4.3 View

3.3.4.3.1 Toolbar

Turns on/off the toolbar.

3.3.4.3.2 Status Bar

Turns on/off the status bar at the bottom.

3.3.4.3.3 Columns

Turns on/off columns in the Mail Jail

- **Icon** - Graphical indication of the type of message
- **Status** - Shows an icon for actions taken on the message. See the Legend.
- **Score** - Total spam score as assigned by the Analyzers for the message
- **Account** - The account to which the e-mail was delivered.
- **To** - The e-mail address to which the e-mail was addressed (not always the same as the account).
- **From** - The e-mail address of the sender (as reported by the e-mail message which can be faked).
- **Analyze Date** - The date and time that the message was analyzed by Spam Sleuth.
- **Email Date** - The date and time the message was sent as reported by the e-mail (can be faked).
- **Size** - The size of the message including unencoded attachments.
- **Subject** - The subject of the message as extracted from the e-mail message.

3.3.4.3.4 Display

Hides or shows the messages of certain types.

- **Still on Server** - Messages that are still on the server. This means different things depending on the mode.
- **Good** - Messages that fell below the spam score when analyzed.
- **Modified** - Messages that were modified by analyzers like HTML Removal, Attachments which can modify the message to make is safer.
- **Spam** - Messages that exceeded the spam score when analyzed.

3.3.4.3.5 View Message

Views the selected message in a safe viewer.

3.3.4.3.6 Legend

Displays the legend for the icons.

3.3.4.4 Help

3.3.4.4.1 Help Topics

Opens the help for the program.

3.3.4.4.2 About...

Shows version number and information about the program.

4 Advanced Features

4.1 Master Files

The Master files are the default files for the entire Enterprise. If you re-install Spam Sleuth Enterprise, all of the existing .MASTER files will remain unchanged.

BadWords.MASTER - The enterprise-wide list of Bad words.

GoodWords.MASTER - The enterprise-wide list of Good words.

Spammers.MASTER - The enterprise-wide list of Spammers.

Friends.MASTER - The enterprise-wide list of Friends.

Score.MASTER - Change the default threshold scores for the entire organization.

```
[General]
DeleteAfter=30
SpamScore=190
StopScore=1000
TrashScore=10200
```

Turing.MASTER - The default Turing settings.

Bouncer.MASTER - The default Bouncer settings.

Profanity.MASTER - This file is not user editable. You can add profanities to an individual's Profanity.INI file and then copy it to Profanity.MASTER.

4.2 Authentication Methods

Spam Sleuth Enterprise supports three authentication methods.

- 1 - Built-In
- 2 - LDAP/Active Directory
- 3 - RADIUS

The Built-In authentication method (1) uses the Unix Crypt MD5 hash method, and you add all of the users either through the Windows Client, the Web Client, or directly to the accounts.conf file.

The LDAP/Active Directory method (2) connects to an LDAP server or Active Directory server to authenticate the users. The Spam Sleuth Enterprise service uses the user list from the LDAP/Active Directory server. You create an ldap.conf file in the /Spam sub-directory which specifies which groups are Spam Sleuth Enterprise users.

The RADIUS method (3) is for authentication only. When the users log in, the password will be authenticated against the RADIUS server. You must have a radius.conf file in the /Spam sub-directory. See the radius.conf.sample file.

See accounts.conf for more information on how use a different authentication method.

4.2.1 accounts.conf File

The accounts.conf file is the account and domain configuration file. We have documented the file format for you, so that you can export accounts from your e-mail program to this file format.

File Format

There are six types of lines.

1) Comment line

You may add comments if you'd like by preceding the line with a # sign. Comment lines may be moved when using the Accounts user interface.

Example:

```
#Executive e-mail addresses start here
```

2) User Account line

user's e-mail followed by the user type (see types). If you specify :R after the user type, RADIUS will be used to authenticate the password, see radius.conf.

Example:

```
joe.jones@thiscompany.com=5  
or  
joe.jones@thiscompany.com=5:R
```

3) Alias Account line

alias e-mail followed by the user's e-mail (The User's Account line must precede the Alias line)

Example:

```
sales@thiscompany.com=joe.jones@thiscompany.com
```

4) Primary Domain line

Domain name preceded by an '@' symbol followed by the authentication type.

Examples:

```
@thiscompany.com=1
```

5) Secondary Domain line

Domain name preceded by an '@' symbol, followed by primary domain (with '@' sign)

Example:

```
@anothercompany.com=@thiscompany.com
```

6) All unknown account line

* followed by either (0, 8, or e-mail address) If no * account exists, then a 550 error will be returned for unknown users.

Examples:

*=0 (all unknown e-mail is relayed to your e-mail server without analysis)

*=8 (Learning mode - all unknown e-mail for domains will be relayed and if successful, an account will be added)

*=joe@acompany.com - (all unknown e-mail will be sent to joe@acompany.com and analyzed by the rules for joe@acompany.com)

User Types (listed in best-to-worst order):

- 1 is Master User (Can add and remove accounts)
- 2 is Regular User (Configuration and Spam View allowed)
- 3 is Regular User (No Configuration allowed)
- 5 is No Spam View, No UnSpam allowed
- 4 is No Config - No Spam View - No Login allowed
- 0 is a passthrough account (no analysis)
- 9 is not active

Sample File:

```
#This company has two domains
@acompany.com=1
@bcompany.com=@acompany.com
joe=1
info=joe
bob@acompany.com=0
bob@bcompany.com=2
sales=bob@bcompany.com
*=8
```

The example above would create these accounts:

joe@acompany.com (primary account to log into - master user)
joe@bcompany.com (alias for joe@acompany.com)
info@acompany.com (alias for joe@acompany.com)
info@bcompany.com (alias for joe@acompany.com)
bob@acompany.com (primary account to log into - passthrough account)
bob@bcompany.com (primary account to log into - regular user)
sales@acompany.com (alias for bob@bcompany.com)
sales@bcompany.com (alias for bob@bcompany.com)

All unknown e-mail with domain (...@acompany.com or ...@bcompany.com) would be relayed to the server. If it accepted, then the account would be added to the accounts.conf file.

IMPORTANT ORDERING

- Domains must come before users or aliases without domains.
- Users must come before their aliases.
- Users-with-domain which override the automatic alias creation, must come after the user-without-domain.

4.2.2 ldap.conf

The ldap.conf file is only used if you are using *LDAP/Active Directory* Authentication.

The ldap.conf file is necessary to use *LDAP/Active Directory* Authentication.

Create the ldap.conf file if you want to specify which groups can use Spam Sleuth Enterprise

Start by specifying the LDAP server and group to User Type mapping. This line specifies the rights that users will have when using Spam Sleuth Enterprise based on the *LDAP/Active Directory* groups they belong to.

```
<active directory domain>:<Active Directory Group>=<user type>
```

Example:

```
myactivedirectoryserver.com:EMailUsers=2
```

Then specify the domains that will use LDAP/Active Directory. If your e-mail domain is the same as your LDAP/Active Directory domain, they might be the same (see second example).

```
<@domain>=<active directory domain>
```

Example:

```
@myemaildomain.com=myactivedirectoryserver.com
```

or

```
@mydomain.com=mydomain.com
```

Then specify the alias domains:

```
<@alias domain>=<@domain>
```

Example:

```
@mydomain.com=@maindomain.com
```

Then specify the alias users. The users do not need to be specified, as they will come from the LDAP/Active Directory Server. The alias can be just a user (first example), or fully qualified (second example). If the alias is not fully qualified with a domain, then the alias will exist for all domains you've specified above.

```
<username>=<fully qualified e-mail>
```

Example:

```
sales=joe@mydomain.com
```

or

```
sales@mydomain.com=joe@mydomain.com
```

Sample File:

```
abccompany.local:Domain Admins=1
abccompany.local:SpamSleuthUsers=2
abccompany.local:Secretary Group=2
abccompany.local:Telemarketers=5
@abccompany.com=abccompany.local
@defcompany.com=defcompany.local
@aliascompany.com=@abccompany.com
sales=jim@abccompany.com
info@abccompany.com=jim@abccompany.com
```

Let's say jim is a member of the SpamSleuthUsers domain in the abccompany.local domain, he will have an e-mail account jim@abccompany.com, and another e-mail account as jim@defcompany.com. Also, he will have an alias account jim@aliascompany.com which is accepted by Spam Sleuth Enterprise and sent to jim@abccompany.com. Also, any e-mail sent to sales@abccompany.com, sales@defcompany.com, or sales@aliascompany.com will go to jim@abccompany.com. Any e-mail for info@abccompany.com will go to jim@abccompany.com.

This is a fairly complex example intended to show the power and flexibility of the system and to show the various types of aliases, and users.

Using the sample file above, any member of the "Domain Admins" group in the abccompany.com domain will be a Master User, any member of "Spam Sleuth Users" will be a Regular User, any member of the "Secretary Group" will also be added as a Regular User, and any member of "Telemarketers" will be a No Spam View, No UnSpam allowed user. See accounts.conf for the User Types.

Using the ldap.conf file allows you to use your LDAP, or Active Directory to add users. By adding users to groups, you determine what rights they have in Spam Sleuth Enterprise. If you already have groups of users, just add the groups to the ldap.conf file.

If a user is a member of more than one group, then they will be added as the most powerful user type. The User Type order is 1, 2, 3, 5, 4, 0, 9. See accounts.conf for the User Types.

IMPORTANT ORDERING - General rule: Must appear on left-side before appearing on right-side of equal sign

- Domain:Group=Type lines must be first
- EMail Domain=LDAP/Active Directory domain must be next

- EMail Domain Alias=EMail Domain must be next
- Alias users must be last

4.2.3 radius.conf

The radius.conf file specifies the server, port and shared secret necessary to authenticate against a RADIUS server.

You must specify the server (by IP), the port, and the shared secret. Put a **:R** after the User Type in the accounts.conf file to specify that the user should be authenticated with RADIUS, instead of the Built-In authentication.

radius.conf.sample file

```
-----  
# The IP address or hostname of the radius server  
server=a.b.c.d  
#  
# The port of the radius-server, if it is zero it will take the  
# one specified in /etc/services. 1645 is a well known one.  
#  
port=1645  
#  
# Shared secret for the server  
#  
secret=sharedsecret  
#  
# Whether to send the domain when authenticating  
# 0 - Send john_doe    1 - Send john_doe@domain.com  
# If usedomain is not set, then it defaults to 1  
#  
usedomain=1
```

4.3 domainrelay.conf File

This is an advanced feature that can relay e-mail to different e-mail servers depending on the domain of the RCPT TO:. To use this file, you must set the "Relay to Host" in SSConfig.exe to "domainrelay"

Format:

```
<domain>=<host>[:<port>]
```

If the optional port is not supplied, it will default to the standard SMTP port of 25.

You may specify the host by IP or by name. If you specify the host by name, make sure that the computer has sufficient DNS Server information to resolve the name to an IP address.

You should set a "default" for any RCPT TO: domains that are not listed. If you leave the "default" blank, it will use the host from the first line as the default.

Sample domainrelay.conf file:

```
abc.com=10.7.4.22  
def.com=mailserver.def.com  
default=10.7.4.13:2500
```

4.4 Learning Mode

Learning Mode lets your Spam Sleuth Enterprise server learn accounts as they come in. We don't recommend that you run in this mode all the time, but rather use it for the first several weeks to automatically add valid accounts.

Make sure that your e-mail server is properly configured, and will reject unknown e-mail with a 550 error. A 550 error is the standard SMTP error ([RFC 821](#)) for rejecting e-mail sent to unknown users.

Go to Accounts to set Learning Mode, and your Domain(s).

When a new e-mail arrives:

1. Spam Sleuth Enterprise will automatically reject e-mail not belonging to your domain.
2. If the account exists, the message will be analyzed and relayed if it is not spam.
3. If the account does not yet exist, your e-mail server will be queried to determine if the user account is valid. If the user account is valid, the account will be created, and added to the accounts.conf file. If the account is not valid, a 550 error will be returned to the sender.

By default, the user account will be added as just a user without the domain, but you may change the default behavior by editing the SpamSleuthServer.INI file in the /Server directory.

SpamSleuthServer.INI

[General]

LearnUserType=2 ;Default user type (see accounts.conf)

LearnUserWithDomain=0 ;Defaults to learning with username only, so Primary and Secondary domains will create user login and aliases. Set to 1 to create user account for each domain.

Only set these if you want Spam Sleuth Enterprise to learn the users from a different server. This could be useful, if you have a database of users. You could write a custom application that responds with a 250 if the user is valid and 550 if the user is invalid.

[General]

LearnHost=<RelayHost>

LearnPort=<RelayPort>

4.5 Restrictions

To use the Restrictions, add a Restrictions.INI file to your \\SERVER\SLEUTH\SPAM directory

The following example will remove Blacklists and Score configuration from everyone (except Master Users), and Joe won't be able to access Bayesian or Turing, but will be able set Score thresholds.

RESTRICTIONS.INI

[Default]

Blacklists=0

Score=0

[joe@mycompany.com]

Bayesian=0

Turing=0

Score=1

Rules:

- If the file is empty or missing there are no restrictions
- The restrictions do not apply to Master Users
- Use the name of the Analyzer file (without the .analyzer extension)

- You can use 'Score=0' even though there isn't a Score.Analyzer file
- The Default applies to all non-Master users and the individual setting override the default
- Setting to "=0" turn it off, setting it to "=1" turns it back on.

[General]

AllowUserToggle=0 ;Set to 1 to allow Master Users to toggle between users in Web Client

4.6 Score and Store

If you turn on the Score and store non-spam in the Miscellaneous section of Configure..., Spam Sleuth will keep a record of all the green dotted messages received and you can view the score and store report in the Mail Jail. This feature comes in handy because sometimes-real messages are indeed spam, and you can view the Score and Store report to better configure Spam Sleuth so that you don't receive messages from that Spammer again. You can right-click and "Add to Spammers" to keep messages with the same From: address from making it into your InBox. For more information about the Score and Store report see the Interface section.

Spam Sleuth™ is very customizable. It has been tuned to work right out of the box. You will be able to get better performance by configuring the program for the type of e-mail that you receive.

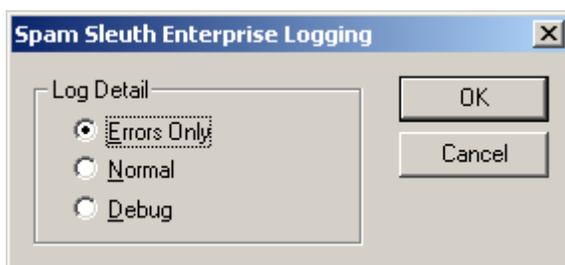
Spam Sleuth displays color coded dots next to the messages in the Mail Jail.

- Red – indicates the e-mail is spam
- Yellow – indicates the e-mail is not spam but has been modified. For example, you may have received an HTML e-mail, and Spam Sleuth stripped out all of the HTML and routed a text version of the message to your inbox.
- Green – indicates that the total amount of points the e-mail received from the Analyzers scored less than the spam threshold. For information about the threshold settings and analyzers see the Defeating Spam section in this manual.
- Green on Yellow - indicates that the message is still on the server. This has different meanings depending on the mode the account is in.

4.7 Logging

Spam Sleuth has the ability to log information which can be helpful in identifying configuration problems.

Open Spam Sleuth and hit CTRL-ALT-L to set the logging level.



Errors Only – Logs errors for use in tracking problems.

Normal – Logs information about start-up, accounts and shut-down.

Debug – Logs the detail of the conversations between e-mail programs and servers. Passwords are not logged even in debug level.

4.8 Server Logging

There are four different logging options in Spam Sleuth Enterprise

Server Logging

This will log the inbound connections, analyzer loading, any analyzer problems, etc. There are three levels you can choose from:

- **Errors Only** - Logs only errors and problems you should be aware of
- **Normal** - Logs some additional information that may be interesting
- **Debug** - Logs inbound conversations, analyzer loading and unloading, reloading of accounts and other information that may be useful in determining the cause of unexpected problems.

You can turn on Server Logging from SSConfig.

Relay To Host Logging

Under normal circumstances, the conversation between Spam Sleuth Enterprise and your internal e-mail server will not need logging. If there is a problem you can log the conversation so you can diagnose any problems.

Client Logging

The Windows client can Unspam messages, add to Friends, Train the Bayesian Analyzer and more. If there is a problem with the client, you can turn on logging by first logging into the client and then hitting CTRL-ALT-L and set the logging level. The log file will be `\\Server\Sleuth\Spam\[user]\SpamSleuth.log`. Each user will have their own log file in their own directory.

Statistics Logging (Reporting)

The server can log in formats that you can use to analyze the spam-to-good ratio, number of e-mails, analysis speed and more. The formats are compatible with web log trend analysis software such as WebTrends from [NetIQ](#), or [SawMill](#), and [many more](#).

To turn on Statistics Logging, add `StatisticsLogging=1` to the `SpamSleuthServer.INI` in the `\Server` directory. The log location will be `\Server\StatLog`

The default is to log in the Extended Log Format. (`StatisticsLoggingFormat=E`). The files will be `exYYMMDD.log`.

You can also log statistics in the Common Log Format by setting `StatisticsLoggingFormat=C` in the `[General]` section of `SpamSleuthServer.INI`. The files will be `ssYYMMDD.log`.

The default is to log detail for aliases. If you don't want to log the detail for aliases, add this line to the `SpamSleuthServer.INI` in the `\Server` directory.

```
[General]
StatisticsLoggingAliases=0
```

If you would like to log to a different location, you can add this line to the `SpamSleuthServer.INI` in the `\Server` directory:

```
[General]
StatisticsLoggingDir=[fully qualified path]
```

4.8.1 Extended Log Format

date - See format below
time - See format below (24 hour time format)
c-ip - Client IP address
cs-username - MAIL FROM: no '<' or '>'
s-ip - Server Receiving IP address
s-port - Server Receiving Port
cs-uri-stem - User[/Alias]/Status
sc-status - 550 (rejected), 404 (spam), 200 (good)
sc-bytes - Number of bytes received (size of e-mail message before analyzing)
time-taken - Time in seconds from start of connection to the end-of-relay disconnect
cs(Referrer) - The information sent during HELO
x-score - The score that the e-mail received

SAMPLE:

```
#Software: Spam Sleuth Enterprise
#Version: 1.0
#Date: 2003-06-03 14:29:28
#Fields: date time c-ip cs-username s-ip s-port cs-uri-stem sc-status sc-bytes time-taken cs(Referrer)
x-score
2003-06-03 14:29:28 207.86.139.145 bob@outside.com 10.7.4.219 25
jim@inside.com/sales@inside.com/good 200 10832 1.023 IMS+Server+[10.1.1.145] 189
```

4.8.2 Common Log Format

No header - Fields are in this order:

host - IP address of the computer sending the e-mail
ident - RFC931 (identity info reported by client) - Not Used
authuser - (Authenticated user - We use it for MAIL FROM: without < or >)
date - [01/Jan/1997:13:06:51 -0600]
request - User[/Alias]/Status
status - 550 (rejected), 404 (spam), 200 (good)
bytes - Number of bytes received (size of inbound message file before analyzing)

SAMPLE:

```
207.86.139.145 - bob@outside.com [13/Jun/2003:14:29:28 -0600]
jim@inside.com/sales@inside.com/good 200 10832
```

4.9 E-mail client relay

Spam Sleuth Enterprise will not allow any e-mail relaying by default. You can tell Spam Sleuth Enterprise to relay e-mail for certain IP addresses. Usually this will be your internal IP addresses of your user's computers.

If you are using a second computer for Spam Sleuth Enterprise, you shouldn't need an access.conf file. If you are using Spam Sleuth Enterprise on the same computer as your e-mail server, and you don't want to change the port that the e-mail clients use to send e-mail, you can add the access.conf file.

Create a file named access.conf in the \Server directory. In most cases, you would just need to add your internal e-mail addresses like this:

```
relay <subnet> <mask>
```

Example:

```
relay 10.1.1.0 255.255.255.0
```

This would cause any e-mail sent from any IP starting with 10.1.1.x to be relayed directly from Spam Sleuth Enterprise to the e-mail server specified in "Relay to Host"

You can also specify to analyze e-mail from an IP range:

```
analyze <subnet> <mask>
```

Example:

```
analyze 10.1.1.2 255.255.255.255
```

This will analyze any e-mail sent from the single IP address 10.1.1.2.

You can have Spam Sleuth Enterprise reject e-mail from an IP range. This may be useful, if you find that you only spam from certain IP ranges:

```
reject <subnet> <mask>
```

Example:

```
reject 209.220.10.0 255.255.255.0
```

This will reject any e-mail for the Class C subnet of 209.220.10.x. Any e-mail from that Class C range would be rejected. Spam Sleuth Enterprise would close the connection immediately.

Below is an example where you would like to allow all of your internal users to relay e-mail, but you want any inbound e-mail relayed from your firewall to be analyzed. Spam Sleuth Enterprise will use the first one that matches. If the e-mail came in as 10.1.1.2, then it would match the first line and be analyzed. If the e-mail came in from 10.1.1.3, then it would match only the second line and be automatically relayed. If an e-mail came in from 209.220.10.4, the connection would be immediately severed.

```
analyze 10.1.1.2 255.255.255.255
relay 10.1.1.0 255.255.255.0
reject 209.220.10.0 255.255.255.0
```

Important: The default is to analyze everything, so there is no reason to put an `analyze` line at the bottom. The message will only be analyzed if it meets all the other criteria such as a valid user in a valid domain, etc. See Configuration-Accounts for user and domain options, and how Spam Sleuth Enterprise will handle unknown users and domains.

4.10 Hidden Server Settings

To change the text that is reported by Spam Sleuth Enterprise during the SMTP connection:

In the `/Server/SpamSleuthServer.INI` file

```
[General]
```

```
SMTPTag=Blue Squirrel SMTP
```

The default is to change the RCPT TO: from the alias address to the user address. This allows you to license Spam Sleuth Enterprise for fewer users. If you choose to turn this off, then each alias will be

considered a user for purposes of licensing.

[General]

AliasRCPTTO=1 ;Setting to 0 will cause Spam Sleuth Enterprise to relay using exactly the same address that it received.

To allow Master Users the ability to quickly toggle to all accounts by simply choosing a user from a drop-down, add this line to the Restrictions.INI in the Spam sub-directory:

[General]

AllowUserToggle=1

To automatically notify new users that Spam Sleuth Enterprise is available for them, set this option in the /Server/SpamSleuthServer.INI file. See New User Notification for the message that is sent.

[General]

NewUserNotify=1

To keep ultra-large messages from overwhelming a server, you can set this setting.

[General]

MaxMessageSize=<bytes>

4.10.1 New User Notification

The text for the new user notification: See Hidden Server Settings to turn it on.

To: [::EMAIL::]

From: [::PROGRAM::]

Subject: Your resource for controlling junk e-mail

This e-mail message is to notify you that your e-mail is being analyzed by an anti-spam program. The benefit to you is that junk e-mail will be filtered out saving you time and allowing you to be more productive.

The anti-spam program [::PROGRAM::] is able to filter out most junk e-mail with no tuning. You may wish to tune it so that you will always get e-mail from certain people, or to block certain e-mails that get through and shouldn't.

To tune [::PROGRAM::] or see the junk e-mail that was caught by

[::PROGRAM::], run [::PROGRAM::] from here:

[::LOCATION::]

Log in with:

E-mail: [::EMAIL::]

Password: [::PASSWORD::]

The best tuning you can do is to add your Friends, and GoodWords.

ADDING FRIENDS

Run [::PROGRAM::], and choose File->Configure... and then Friends. Add the e-mail address of your friends. You may see some listed already. These are configured by the administrator for everyone.

ADDING GOODWORDS

Run [::PROGRAM::], and choose File->Configure... and then GoodWords. Add words that pertain to your job. For example: If you work at a tire

company, you would add words like 'Tread', 'Skid', 'Traction', 'Michelin', etc.

There are many other options for tuning [::PROGRAM:], see the Help for more information.

4.11 Command Line Options

You can add options to the command line of Spam Sleuth to cause it to behave differently. To add a command line go to your Windows Start menu > Programs > Startup > right-click on the Spam Sleuth icon > Properties. Select the Shortcut Tab, and in the Target section you can add any of the following characters to the end of the address. Ensure that you leave a blank space after .exe and the start of your command line /NoSplash.

- **/NoSplash** – This option keeps the Splash Screen from appearing on start up.
- **/User:<user> /PASS:<pass>** - Log in the specified user.

4.12 Tips and Tricks

4.12.1 Shortcut Keys

You can use the following shortcut keys to access features quickly without menus or using your mouse. Spam Sleuth must be active and the MailJail window must be open.

- **ESC** – Minimizes the MailJail window.
- **F5** - Refresh messages from server
- **F4** – Changes the active account in the MailJail.
- **CTRL-M** – Checks e-mail in the active account.
- **ALT-U** - 'U'nSpam a message
- **ALT-G** - Mark a message as 'G'ood
- **CTRL-ALT-L** – Set the logging level. The log is stored in the same directory as the program, and is named SpamSleuth.LOG. For efficiency, a new log file will be created when log becomes too large. The old log file will be named SpamSleuth.1.LOG.

4.12.2 Positive Tuning

Positive Tuning is making sure that the e-mail you want to receive is able to make it through to your InBox and will not be tagged as spam. Here are some recommendations.

- Add all your friends and co-workers to the Friends list.
- Add any mailing lists to which you subscribe to the Friends list.
- Add any topic that you are interested in to the GoodWords list. This may include sports, hobbies, services, product names, people's names, etc.

Once you've done this, then you can go to the Score analyzer configuration and lower the spam score. This will catch more spam. If you've done a good job with the positive tuning, your desirable e-mail will be getting through and the spam will be kept out.

Twice a week, or at your leisure, open the Mail Jail and sort by Score. Quickly scan for e-mails that are not spam. Usually these will have a low score. If the sender should be on your Friends list, just right-click and Add to Friends.

For each desirable e-mail that was tagged as spam, look to see if there are identifying characteristics that you can use so that you get the message in the future. The easiest is, of course, to add the sender to the Friends list. There may be a better way. Perhaps you can add the entire domain to the Friends list, or add a GoodWord that will let similar messages reach you in the future.

The goal of positive tuning is to find out why friends and non-spam were rejected and fix it without allowing an easy way in for spammers.

4.12.3 Negative Tuning

- Once you've done the positive tuning, watch for spam coming into your InBox. Look at the e-mail and see if it could've been tagged as spam.
- Does it have spam-like words? -> Add to the BadWords.
- Do you get lots from the same e-mail or domain? -> Add the e-mail or domain to Spammers.
- Do they use lots of HTML? -> Increase the points for HTML formatting.
- Do they use loud HTML (reds, yellows, large fonts)? -> Increase the max points or sensitivity in HTML Volume.
- Did one of the analyzers find something? -> Increase the points for that if it won't knock out your good e-mail.
- Are profane e-mails getting through? -> Increase the points for Profanity.

5 Customer Support

This User's Manual focuses on your specific needs, supplying most of what you need to know to be productive with Spam Sleuth™. Below we have listed several options to choose from to assist you with any help you may need using Spam Sleuth™. Additional information about Spam Sleuth™ can be found in the README file.

5.1 Spam Sleuth Help File

To access the Spam Sleuth™ help file, click Help > Help Topics. We encourage you to use the Spam Sleuth™ help, because it's a complete, informative reference system. In addition, Help offers several advantages over the printed manual.

In the Help Index, you can type in a keyword, and the program automatically looks it up for you. While reading the Help file you can click on a "hot" phrase to jump to a related topic. And later you can retrace your steps; flipping backwards through the topics you jumped from. Or you can read topics in order, like turning the pages of a book, either forward or backward.

5.2 How to Find Specific Topics in the Help File

The Help system displays both the Contents and Index lists, providing alternative ways to get information pertaining to a specific topic. The list of Contents shows the major categories of Help. When a category is chosen, you'll be presented with Help text directly, or a pop up menu of topics, from which your choices will be narrowed. The index allows you to look up a word or phrase you have in mind. Type the word or phrase, or look in the alphabetical list for your topic, select it, and click Display.

Clicking on the highlighted word or phrase brings up a list of Associated Topics. Double click on any associated topic to read the contents. Or double click on the word or phrase to go directly to its first associated topic.

If you prefer to browse or read straight through Help, go to any topic as a starting point. From there, use the >> and << buttons to move through topics forward or backward. You can read through the entire Help system in this way.

5.3 Visit Our Web Site

Program Web Site:

<http://www.bluesquirrel.com/products/SpamSleuthEnterprise/>

If you cannot find the information you need at the program web site, try our FAQs located in our Technical Support area for assistance.

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

5.4 Technical Support

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

5.5 Customer Service

You're more than welcome to contact us via telephone. If you would like to speak with a Blue Squirrel representative regarding non-technical issues please select from the following options:

Phone: 801-352-1551

Toll Free: 800-403-0925

Fax: 801-912-6032

E-mail: sales@bluesquirrel.com

Note: Hours are: Monday through Friday, 8:00 a.m. to 5:00 p.m. Mountain Standard Time.

5.6 Mailing address

Blue Squirrel
686 E. 8400 South
Sandy, UT 84070

6 Reference

6.1 Glossary

APOP – Authenticated POP – a way of sending the password to the incoming e-mail server in an encrypted way so that it cannot be retrieved by network sniffers. Only some POP3 servers support this feature. You can test it with the POP3 Test button.

ASMTTP – Authenticated Simple Mail Transfer Protocol – A specification for sending user and password information to an SMTP server. See SMTP. The original SMTP did not allow for authentication.

Blacklists – Blacklists keep track of the IP addresses of known spam servers, and open relay machines that can assist spammers. Spam Sleuth can check with these servers to determine whether an e-mail was sent from a known spam server.

Charsets – E-mail programs can specify a non-standard character set which is usually used for Chinese and Korean e-mails. E-mails that use other character sets can show additional characters. Spam Sleuth allows you to add points for these characters and also for e-mails that specify different character sets.

Common Log Format - An industry standard log format as defined by the [W3C](#).

ESMTTP – Extensions to Simple Mail Transfer Protocol – A specification for additional features beyond SMTP. See SMTP. ESMTTP servers can support additional login methods.

Extended Log Format - An industry standard log format as defined by the [W3C working draft \(WD-logfile\)](#).

IMAP4 – A protocol based on [RFC 1730](#) that allows downloading messages as well and putting messages into folders on an e-mail server. Most ISPs use POP3 instead of IMAP4. Most servers that support IMAP4 also support POP3. Spam Sleuth uses POP3 and not IMAP4.

Polling Mode – The mode in Spam Sleuth which is the opposite of POP3 Proxy Mode. In Polling Mode, Spam Sleuth must check your e-mail before your e-mail program. Any non-spam messages will be left on your e-mail server, while spam messages will be removed and temporarily stored.

POP3 – Post Office Protocol 3 – A specification for an e-mail server to talk to an e-mail client. Based on [RFC 1939](#), POP3 specifies how an e-mail program like Eudora, or Outlook communicate with a server to get the e-mail.

POP3 Proxy Mode – The mode in Spam Sleuth which when activated in account configuration will cause Spam Sleuth to become your e-mail server. You must modify two settings in your e-mail program when using POP3 Proxy Mode. Change the Incoming (POP3)

Server to localhost, and change the login/username to your full e-mail address.

Regular Expressions – A very powerful syntax for searching for complex patterns in texts such as e-mail messages. The syntax of the regular expressions used in Spam Sleuth can be found in Appendix A.

SMTP – Simple Mail Transfer Protocol – A specification for an e-mail client to send e-mail to a server, or for an e-mail server to send e-mail to an e-mail server. Based on [RFC 821](#), SMTP specifies how e-mail is sent.

Turing Test - Named after Alan Turing, it is method of determining whether the sender was a human or a machine. A test is given to the sender which is difficult for a machine, but trivial for a human.

Tag Mode - Tag mode is an Enterprise only option which passes all e-mail through, but adds an "X-Text-Classification: spam" header to every spam message. This can be used by the e-mail clients to put the spam into a Junk/Spam folder.

VIP Key - An unlock code that you should have if you've purchased the program. It is usually e-mailed to you if you purchased online. It should also be on the CD or the Manual if you have the hard copy.

6.2 Appendix A (Regular Expression Syntax)

This section covers the regular expression syntax used by Spam Sleuth's Power Filter when using regular expressions for matching strings.

Literals

All characters are literals except: ".", "*", "?", "+", "(", ")", "{", "}", "[", "]", "^", "\$" and "\". These characters are literals when preceded by a "\". A literal is a character that matches itself.

Wildcard

The dot character "." matches any single character except '.'

Repeats

A repeat is an expression that is repeated an arbitrary number of times. An expression followed by "*" can be repeated any number of times including zero. An expression followed by "+" can be repeated any number of times, but at least once. An expression followed by "?" may be repeated zero or one times only. When it is necessary to specify the minimum and maximum number of repeats explicitly, the bounds operator "{}" may be used, thus "a{2}" is the letter "a" repeated exactly twice, "a{2,4}" represents the letter "a" repeated between 2 and 4 times, and "a{2,}" represents the letter "a" repeated at least twice with no upper limit. Note that there must be no white-space inside the {}, and there is no upper limit on the values of the lower and upper bounds. All repeat expressions refer to the shortest possible previous sub-expression: a single character; a character set, or a sub-expression grouped with "()" for example.

Examples:

"ba*" will match all of "b", "ba", "baaa" etc.

"ba+" will match "ba" or "baaaa" for example but not "b".

"ba?" will match "b" or "ba".

"ba{2,4}" will match "baa", "baaa" and "baaaa".

Non-greedy repeats

Whenever the "extended" regular expression syntax is in use (the default) then non-greedy repeats are possible by appending a '?' after the repeat; a non-greedy repeat is one which will match the *shortest* possible string.

For example to match html tag pairs one could use something like:

```
"<\s*tagname[^\>]*>(.*?)<\s*/tagname\s*>"
```

In this case \$1 will contain the text between the tag pairs, and will be the shortest possible matching string.

Parenthesis

Parentheses serve two purposes, to group items together into a sub-expression, and to mark what generated the match. For example the expression "(ab)*" would match all of the string "ababab".

Non-Marking Parenthesis

Sometimes you need to group sub-expressions with parenthesis, but don't want the parenthesis to spit out another marked sub-expression, in this case a non-marking parenthesis

(?:expression) can be used. For example the following expression creates no sub-expressions:

```
"(?:abc)*"
```

Forward Lookahead Asserts

There are two forms of these; one for positive forward lookahead asserts, and one for negative lookahead asserts:

"(?:=abc)" matches zero characters only if they are followed by the expression "abc".

"(?:!abc)" matches zero characters only if they are not followed by the expression "abc".

Alternatives

Alternatives occur when the expression can match either one sub-expression or another, each alternative is separated by a "|". Each alternative is the largest possible previous sub-expression; this is the opposite behavior from repetition operators.

Examples:

"a(b|c)" could match "ab" or "ac".

"abc|def" could match "abc" or "def".

Sets

A set is a set of characters that can match any single character that is a member of the set. Sets are delimited by "[" and "]" and can contain literals, character ranges, character classes, collating elements and equivalence classes. Set declarations that start with "^" contain the compliment of the elements that follow.

Examples:

Character literals:

"[abc]" will match either of "a", "b", or "c".

"[^abc]" will match any character other than "a", "b", or "c".

Character ranges:

"[a-z]" will match any character in the range "a" to "z".

"[^A-Z]" will match any character other than those in the range "A" to "Z".

Note that character ranges are highly locale dependent: they match any character that collates between the endpoints of the range, ranges will only behave according to ASCII rules when the default "C" locale is in effect. For example if the library is compiled with the Win32 localization model, then [a-z] will match the ASCII characters a-z, and also 'A', 'B' etc, but not 'Z' which collates just after 'z'.

Character classes are denoted using the syntax "[:classname:]" within a set declaration, for example "[[:space:]]" is the set of all whitespace characters. The available character classes are:

alnum	Any alpha numeric character.
alpha	Any alphabetical character a-z and A-Z. Other characters may also be included depending upon the locale.
blank	Any blank character, either a space or a tab.
cntrl	Any control character.
digit	Any digit 0-9.
graph	Any graphical character.
lower	Any lower case character a-z. Other characters may also be included depending upon the locale.
print	Any printable character.
punct	Any punctuation character.
space	Any whitespace character.
upper	Any upper case character A-Z. Other characters may also be included depending upon the locale.
xdigit	Any hexadecimal digit character, 0-9, a-f and A-F.
word	Any word character - all alphanumeric characters plus the underscore.
unicode	Any character whose code is greater than 255, this applies to the wide character traits classes only.

There are some shortcuts that can be used in place of the character classes:

\w in place of [:word:]

\s in place of [:space:]

\d in place of [:digit:]

\l in place of [:lower:]

\u in place of [:upper:]

Collating elements take the general form [.tagname.] inside a set declaration, where *tagname* is either a single character, or a name of a collating element, for example [[.a.]] is equivalent to [a], and [[.comma.]] is equivalent to [,]. The library supports all the standard POSIX collating element names, and in addition the following digraphs: "ae", "ch", "ll", "ss", "nj", "dz", "lj", each in lower, upper and title case variations. Multi-character collating elements can result in

the set matching more than one character, for example `[.ae.]` would match two characters, but note that `^[.ae.]` would only match one character.

Equivalence classes take the general form `[=tagname=]` inside a set declaration, where *tagname* is either a single character, or a name of a collating element, and matches any character that is a member of the same primary equivalence class as the collating element `[.tagname.]`. An equivalence class is a set of characters that collate the same, a primary equivalence class is a set of characters whose primary sort key are all the same (for example strings are typically collated by character, then by accent, and then by case; the primary sort key then relates to the character, the secondary to the accentation, and the tertiary to the case). If there is no equivalence class corresponding to *tagname*, then `[=tagname=]` is exactly the same as `[.tagname.]`.

To include a literal "-" in a set declaration then: make it the first character after the opening "[" or "[^", the endpoint of a range, or a collating element.

Line anchors

An anchor is something that matches the null string at the start or end of a line: `^` matches the null string at the start of a line, `$` matches the null string at the end of a line.

Back references

A back reference is a reference to a previous sub-expression that has already been matched, the reference is to what the sub-expression matched, not to the expression itself. A back reference consists of the escape character `\` followed by a digit "1" to "9", `\1` refers to the first sub-expression, `\2` to the second etc. For example the expression `(.*)\1` matches any string that is repeated about its mid-point for example "abcabc" or "xyzxyz". A back reference to a sub-expression that did not participate in any match, matches the null string: NB this is different to some other regular expression matchers.

Characters by code

This is an extension to the algorithm that is not available in other libraries; it consists of the escape character followed by the digit "0" followed by the octal character code. For example `\023` represents the character whose octal code is 23. Where ambiguity could occur use parentheses to break the expression up: `\0103` represents the character whose code is 103, `(\010)3` represents the character 10 followed by "3". To match characters by their hexadecimal code, use `\x` followed by a string of hexadecimal digits, optionally enclosed inside `{ }`, for example `\xf0` or `\x{aff}`, notice the latter example is a Unicode character.

Word operators

`\w` matches any single character that is a member of the "word" character class, this is identical to the expression `[[:word:]]`.

`\W` matches any single character that is not a member of the "word" character class, this is

identical to the expression "[^[:word:]]".

"\<>" matches the null string at the start of a word.

"\>" matches the null string at the end of the word.

"\b" matches the null string at either the start or the end of a word.

"\B" matches a null string within a word.

The start of the sequence passed to the matching algorithms is considered to be a potential start of a word.

Buffer operators

"\" matches the start of a buffer.

"\A" matches the start of the buffer.

"\" matches the end of a buffer.

"\z" matches the end of a buffer.

"\Z" matches the end of a buffer, or possibly one or more new line characters followed by the end of the buffer.

Escape operator

The escape character "\" has several meanings.

Inside a set declaration the escape character is a normal character.

The escape operator may introduce an operator for example: back references, or a word operator.

The escape operator may make the following character normal, for example "*" represents a literal "*" rather than the repeat operator.

Single character escape sequences

The following escape sequences are aliases for single characters:

Escape sequence	Character code	Meaning
\a	0x07	Bell character.
\f	0x0C	Form feed.
\n	0x0A	Newline character.
\r	0x0D	Carriage return.
\t	0x09	Tab character.
\v	0x0B	Vertical tab.
\e	0x1B	ASCII Escape character.
\odd	Odd	An octal character code, where <i>dd</i> is one or more octal digits.
\xXX	0xXX	A hexadecimal character code, where XX is one or more hexadecimal digits.
\x{XX}	0xXX	A hexadecimal character code, where XX is one or more hexadecimal digits, optionally a unicode character.
\cZ	z-@	An ASCII escape sequence control-Z, where Z is any ASCII character greater than or equal to the character code for '@'.

Miscellaneous escape sequences:

- \w Equivalent to [[:word:]].
- \W Equivalent to [^[:word:]].
- \s Equivalent to [[:space:]].
- \S Equivalent to [^[:space:]].
- \d Equivalent to [[:digit:]].
- \D Equivalent to [^[:digit:]].
- \l Equivalent to [[:lower:]].
- \L Equivalent to [^[:lower:]].
- \u Equivalent to [[:upper:]].
- \U Equivalent to [^[:upper:]].
- \C Any single character, equivalent to '.'.
- \X Match any Unicode combining character sequence, for example "a\x 0301" (a letter a with an acute).
- \Q The begin quote operator, everything that follows is treated as a literal character until a \E end quote operator is found.
- \E The end quote operator, terminates a sequence begun with \Q.

What gets matched?

The regular expression library will match the first possible matching string.

*Regular Expression documentation was modified by Blue Squirrel with permission. The following message applies to the regular expression matching library:
Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Dr John Maddock makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.
Copyright Dr. John Maddock 1998-2000 all rights reserved.*

6.3 Appendix B (Advanced Filter Syntax)

If you are using the Basic Filter, you don't need to use this syntax.

Boolean and other search logic are rich and complex topics which often take up a full semester of a college-level course. Obviously, a full explanation is beyond the scope of this Appendix. However, most Web searches do not require a full range of Boolean expressions but rely on a limited subset of the possible queries.

In this section, we present some examples of valid expressions in both standard English and their search syntax counterparts. The syntax examples given here could be all or part of an expression entered in the Query text box of WebSeeker's Advanced Refine dialog.

Individual Word Searches

To search for the word "shark," simply enter it as is:

```
shark
```

Phrase Searches

To search for the phrase "great white shark," use parenthesis and quotes:

```
("great white shark")
```

That last search looks for all three words in the order shown with no intervening words. Sometimes you would like to maintain the specified ordering but are willing to accept intervening words. To find "men are attacked by the great white shark," you could type the following which allows 3 words between each pair of words:

```
("men attacked shark :3")
```

Of course, the above phrase would also find something like "men are attacking and killing sharks."

Sometimes, because you're unsure of all of the words in a phrase, you may wish to specify that one or more of the words in the phrase are "expendable." For example, the following example specifies that any two of the words specified may be missing and still cause a match:

```
("men and women are attacked and killed by sharks :3:2")
```

If the default span of zero is desired, the previous expression could be entered as:

```
("men and women are attacked and killed by sharks ::2")
```

Proximity Searches

To find two or more words "near" each other but in any order, use a proximity search. For example enter:

```
[taxes deductions]
```

This finds ".taxes after all the deductions.." as well as ".deductions figured from state taxes..."

The brackets indicate that you want to find the words within a certain span or range. The default width of the span is 20 words. You may override the default: For example, here we make the span 10:

```
[federal deductions taxes :10]
```

You may also specify an expendable count. In the following example, we allow two words to be missing from those specified:

```
[federal and state deductions taxes :10:2]
```

Boolean Searches

To find all documents containing "shark," "whale" or "dolphin" (or any combination thereof), use the vertical bar character:

```
shark | whale | dolphin
```

To find all documents containing both "sea" and "ocean," use the ampersand character:

```
sea & ocean
```

Nested Expressions

Any place that you can use a single word in an expression, you may also use a phrase, proximity, or OR ("|") sub-expression. Here are some examples:

```
failed | "gave up"
("deep sea diving | scuba") or equivalently ("deep sea (diving | scuba)")
["cookies and cream" sweets]
(" ("Mother Theresa") ("India") :20")
```

Notice that phrases within phrases require parentheses.

Parentheses

Parentheses may be used to specify the order in which you want the expression to be evaluated. In the following example, we want the AND (&) to be evaluated before the OR (|):

```
(fast & cars) | racing
```

In the next example, we want the OR (|) to be evaluated before the AND (&):

```
Indy 500 & (fast | cars)
```

6.4 License Agreement

THE Blue Squirrel END USER LICENSE AGREEMENT REDISTRIBUTION NOT PERMITTED GRANT.

BY INSTALLING Blue Squirrel SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT INSTALL THE Blue Squirrel SOFTWARE, OR IF YOU HAVE ALREADY INSTALLED IT, UNINSTALL IT IMMEDIATELY.

Subject to payment of applicable license fees, Blue Squirrel grants you a non-exclusive license to use the Software and accompanying documentation ("Documentation") in the manner described below under "Scope of Grant."

SCOPE OF GRANT.

You may:

- use the Software on any single computer;
- use the Software on a network, provided that each person accessing the Software through the network must have a copy licensed to that person;
- use the Software on a second computer so long as only one copy is used at a time;
- copy the Software for archival purposes, provided any copy must contain all of the original Software's proprietary notices;
- or if you have purchased licenses for a 10 pack or a 50 pack, make up to 10 or 50 copies, respectively, of the Software (but not the Documentation), provided any copy must contain all of the original Software's proprietary notices. The number of copies is the total number of copies that may be made for all platforms. Additional copies of Documentation may be purchased.

You may not:

- permit other individuals to use the Software except under the terms listed above;
- permit concurrent use of the Software;
- modify, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), or create derivative works based on the Software;
- copy the Software other than as specified above;
- rent, lease, grant a security interest in, or otherwise transfer rights to the Software; or
- remove any proprietary notices or labels on the software.

LIMITED WARRANTY. Blue Squirrel warrants that for a period of thirty (30) days from the date of acquisition, the Software, if operated as directed, will substantially achieve the functionality described in the Documentation. Blue Squirrel does not warrant, however, that your use of the Software will be uninterrupted or that the operation of the Software will be error-free or secure. In addition, you must determine that the Software sufficiently meets your requirements. Blue Squirrel also warrants that the media containing the Software, if provided by Blue Squirrel, is free from defects in material and

workmanship and will so remain for thirty (30) days from the date you acquired the Software. Blue Squirrel's sole liability for any breach of this warranty shall be, in Blue Squirrel's sole discretion; (i) to replace your defective media; or (ii) to advise you how to achieve substantially the same functionality with the Software as described in the Documentation through a procedure different from that set forth in the Documentation; or (iii) if the above remedies are impracticable, to refund the license fee you paid for the Software. Repaired corrected, or replaced Software and Documentation shall be covered by this limited warranty for the period remaining under the warranty that covered the original Software, or if longer, for thirty (30) days after the date (a) of shipment to you of the repaired or replaced Software, or (b) Blue Squirrel advised you how to operate the Software so as to achieve the functionality described in the Documentation. Only if you inform Blue Squirrel of your problem with the Software during the applicable warranty period and provide evidence of the date you purchased a license to the Software will Blue Squirrel be obligated to honor this warranty. Blue Squirrel will use reasonable commercial efforts to repair, replace, advise, or refund pursuant to the foregoing warranty within 30 days of being so notified.

Index

- A -

accept 76
Access List 13
access.conf 76
Account 17
accounts.conf 69
Active Directory 26, 70
Active Directory Domain 27
Active Directory Groups 27
Add Accounts 23
Add to Friends 62
Add to Spammers 62
Add Users 23
Advanced Filter 88
Alias 24
Aliases 24
AliasRCPTTO 77
Analyze 13, 76
APOP 82
Appendix B 88
ASMTTP 82
Attachments 37
Auto Responder 60
Automatic Login 17

- B -

BadWords 35
BadWords Master 28
Bayes 50
 Thomas 50
Bayesian 48
Bayesian - Advanced Settings 52
Bayesian - Training 51
Bayesian Statistics 52
Blacklist by e-mail 32
Blacklist by IP 43
BlackLists 43, 82
Bounce Method 57
Bouncer 57

- C -

Centralized password 72
Challenge Response 53
Charsets 42, 82
Chinese spam 42
Command Line Options 79
Configuration 10
Configure 17
Configuring 14

- D -

Delete Messages 65
Dictionary 39
Dictionary Master 28
Disable Configuration 73
Domain 23
Domain Admins 70
Domain Relay 72
Drag and Drop 62

- E -

Edit Accounts 23
Edit Users 23
EMail Client Access 13
EMail Sending Blocked 13
EMail Stamp - Sample 57
EMail Stamps 55
ESMTTP 82
Eudora 13, 76
Export - Bayesian Dictionary 48
Export Accounts 69
Extra Text 39

- F -

Filter 65
Friends 30
Friends Master 28

- G -

Getting Started 5

GoodWords 34
 GoodWords Master 28
 Green Dot 63
 Green Dot on Yellow Envelope 63

- H -

Hide Options 73
 HTML Removal 44
 HTML Volume 41
 Human Test 53

- I -

Images 44
 IMAP4 82
 Import - Bayesian Dictionary 48
 Import Accounts 69
 Indexer 65
 Indexing 65
 Install Service 13
 Installation 5
 Introduction 5

- J -

Java 44
 Junk Words 39

- K -

Keep good messages 74
 Korean spam 42

- L -

Launching 14
 LDAP 26, 70
 Learn 50
 Learning Mode 73
 Legend 63
 License Agreement 90
 Licensing 77
 Lightweight Directory Access Protocol 26
 Limit Users 73
 Links 44

LoadAndKeep 14
 Log Format - Common 76
 Log Format - Extended 76
 Logging 74
 Logging - Client 75
 Logging - Relay Conversation 75
 Logging - Reporting 75
 Logging - Server 75
 Logging - Statistics 75

- M -

Mail Jail 61
 Mailing address 81
 Mailing Lists 31
 Manually add accounts 69
 Mark as Good (UnSpam) 65
 Mark as Spam 65
 Master 7, 28
 Master Configuration Files 6, 7, 10
 Master Dictionary 39
 Master files 68
 Master User 12
 Memory Requirements 14
 Modified Message 63

- N -

Naive Bayesian 50
 Negative Tuning 80
 New User 25
 Notify 15

- O -

On-demand configuration loading 14
 Outlook 13, 76
 Outlook Express 13, 76

- P -

Password 17
 Points 20
 Polling Mode 82
 POP3 82
 POP3 Proxy Mode 82
 Positive Tuning 79

Power Filter 48
Power Filter Master 28
Primary Domain 23
Profanity 36
Profanity.MASTER 68

- R -

RADIUS 72
Recycle Bin 65
Red Dot 63
Redirect 59
Reflect 59
Regular Expression 48, 83
Regular Expressions 82
Reject 13, 76
Relay 13, 59
Relay to Multiple Hosts 72
Reporting 75
Restrict Users 73
Restrictions 73

- S -

Score 29
Score and Store 17, 74
Score.MASTER 68
Scripts 44
Searching 65
Secondary Domain 23
Send EMail Blocked 13
Server Configuration 10
Sever Share 12
Shortcut Keys 79
SMTP 82
SMTP Response 77
Sort Columns 61
Spam Viewer 61
Spammers 32
Spammers Master 28
Start 17
Start Service 13
Statistical Analysis 50
Statistics 52, 75
Status 61
Subject 40
Subject Master 28

Suppress Splash Screen 79

- T -

Tag Mode 17
Technical Support 81
Thomas Bayes 50
To 33
Toggle Users 73
Train Bayesian Analyzer 51
Trash 65
Troubleshooting 7, 75
Turing Test 53, 54

- U -

User Configuration Files 6, 10
User Dictionary 39
User Permissions 23
User Rights 23
User Spam Location 6, 10
User Toggle 73
Users 25

- V -

Vacation Responder 60
Valid Sender 46
View All Accounts 61
View Individual Accounts 61
Viewing Spam 14
VIP Key 82
Viruses 37

- W -

Web Bugs 44
Welcome e-mail 16
Whitelist 30
Windows Login 70
Windows Password 70
Word Probabilities 50

- X -

X-Text-Classification 17

- Y -

Yellow Dot 63