Spam Sleuth 4.0

User's Guide

Windows 95/98/ME/NT/2000/XP

Spam Sleuth User's Guide

Printed: June 2004

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

1 Introduction and Getting Started

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

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

Spam Sleuth monitors your e-mail box behind the scenes and automatically analyzes e-mail messages for spam characteristics. Spam Sleuth looks for thousands of different characteristics. It keeps a report of what it finds so that you know why an e-mail has been deemed spam. If Spam Sleuth determines an e-mail is spam, it yanks it off of the e-mail server, compresses it 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.

1.1 Installing Spam Sleuth

1.1.1 System Requirements

- Pentium or faster processor
- Windows 95/98/NT/Me/2000/XP
- 16 MB of RAM
- At least 12 MB hard drive space
- A POP3 e-mail server (provided by most companies and ISPs)
- Requires Web2POP for Hotmail (free), AOL, MSN Web, Yahoo (free), Excite (free)

1.1.2 Installation Summary

The installation setup program is called SpamSleuthSetup.exe. You must run the setup program to install Spam Sleuth ™ to your hard disk (Product installation is found in section "Loading the CD"). Here's a summary of what the setup program does:

- Copies the Spam Sleuth ™ files to your hard disk.
- At the end of the installation process Spam Sleuth ™ presents you with the option to view the README.TXT. We recommend looking this document over because it contains more information about Spam Sleuth ™.

When you first start the Spam Sleuth ™ program, the InstantX registration dialog box will appear. To fully enable your copy of Spam Sleuth ™ please fill out the form and enter your VIP Key, and then send it electronically to Blue Squirrel. If you don't register Spam Sleuth ™ the InstantX dialog box will pop up each time you run the program, and it will run as an evaluation program. Once you have purchased the program and entered your VIP key, you'll

see your License Key code in the About Spam Sleuth ™ box.

1.1.3 Loading the CD

1. Insert the CD into the appropriate disk drive.
2. The CD should automatically load. If the CD does not load automatically, double click on the "My Computer" icon on your desktop. Select your CD drive, go to File on the menu bar and click Open. Find the file named BlueSquirrelInstaller.exe and double click. An introduction screen will appear.

    - Click on the program you would like to install on the left.
    - If you wish to purchase the product click on the BUY text. This will take you to the Blue Squirrel Web purchase page for that product.
    - To demo the product click on the title or on the INSTALL text.

1.2 Registering Electronically

Even if you have not purchased the program, we politely request that you register the program before using the trial. The registration box will appear when you run the program and have not registered. Please ensure that you have an active Internet connection, enter your information, and hit OK. Your information will be sent electronically.

1.3 Registering Manually

Access the InstantX Registration Screen by selecting Help->About Spam Sleuth ™-> InstantX, and then the Settings tab from the Spam Sleuth ™ Menu Bar. Enter in your customer information, and your VIP key and then select the Print button to print the form instead of sending it over the Internet.

Fax the printout to us at 801-912-6032, or send it via post mail to:

Blue Squirrel
Attn. Customer Service
686 E. 8400 South
Sandy, UT 84070

1.4 Purchasing the Program

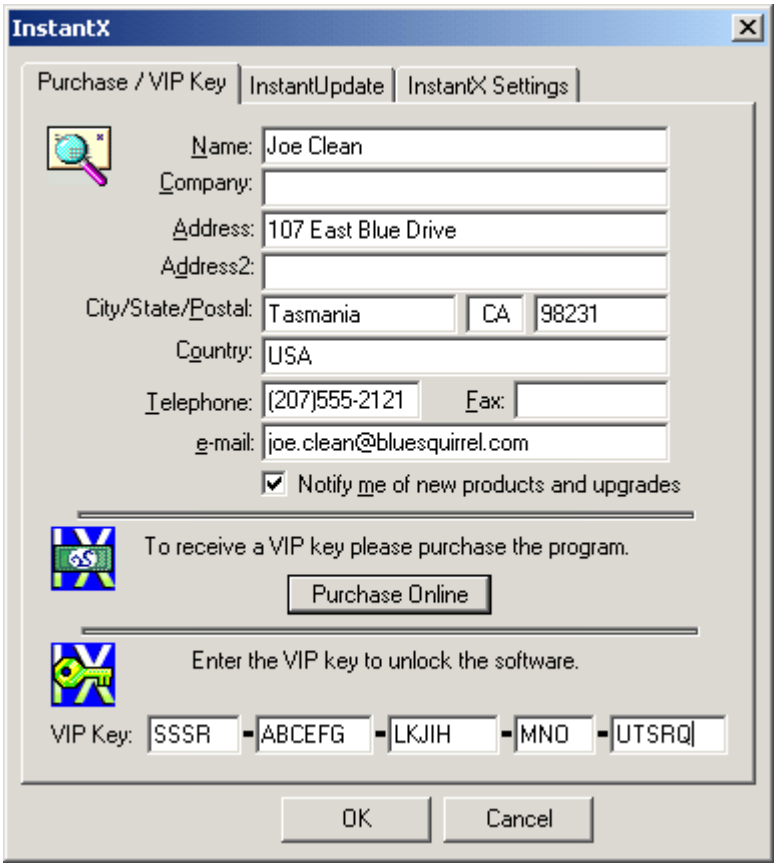
There are many ways to purchase the program. The easiest way is to hit the "Purchase Online" button that will appear each time your start the trial version. You may also call to order the program. We accept all major credit cards.

Once you have purchased the program you will be given a VIP Key. The VIP Key is an activation code to activate the program and remove any trial limitations.

1.5 Activating Spam Sleuth

Make sure you have an active connection to the Internet so you can submit your registration online. The first time you run Spam Sleuth ™, the InstantX Registration dialog box appears. If the InstantX Registration dialog box does not appear you can access it by double-clicking on the Spam Sleuth ™ icon in the System tray, then select Help->About Spam Sleuth ™->InstantX button.
Enter in your customer information, and VIP key, and press OK to submit your information over the Internet.

Your VIP Key looks like this:
SSSR-ABCEFG-LKJIH-MNO-UTSRQP



1.6 Configuration Wizard

1.6.1 POP3 Proxy vs. Polling

Spam Sleuth is able eliminate spam two different ways:

POP3 Proxy Mode and **Polling Mode**

Which is better between '**POP3 Proxy** Mode' and '**Polling** Mode'?

In most cases **POP3 Proxy** Mode is the better mode to use.

POP3 Proxy Mode

Benefits

- Spam Sleuth always analyzes ALL of your messages
- Timing between Spam Sleuth and your e-mail program is not a concern.
- Messages are only downloaded once from your ISP.
- You don't have to store your password with Spam Sleuth .

Disadvantages

- You must change your Incoming (POP3) Server setting in your e-mail program to 'localhost' or 127.0.0.1, but this can be done automatically by the configuration wizard.
- Spam Sleuth must be running for you to get e-mail.

Polling Mode

Benefits

- No configuration of your e-mail program is needed.
- Spam Sleuth doesn't have to be running for your e-mail program to get your e-mail.

Disadvantages

- You must make sure Spam Sleuth analyzes your e-mail before your e-mail program gets your e-mail, or the spam will get through.

What is '**POP3 Proxy** Mode'?

In **POP3 Proxy Mode**, Spam Sleuth will get all of your e-mail from your e-mail server and analyze it. It will separate the spam from the good e-mail and then act as a server for your good e-mail.

In **PO3 Proxy Mode**, Spam Sleuth will set itself up as an e-mail server on the standard POP3 Port of 110 on your local computer. It rejects any attempts to access it from other computers, unless you tell it otherwise. Your e-mail program can access the Spam Sleuth server by configuring your *Incoming Server (POP3)* setting to **localhost**, which is just another name for the IP address 127.0.0.1.

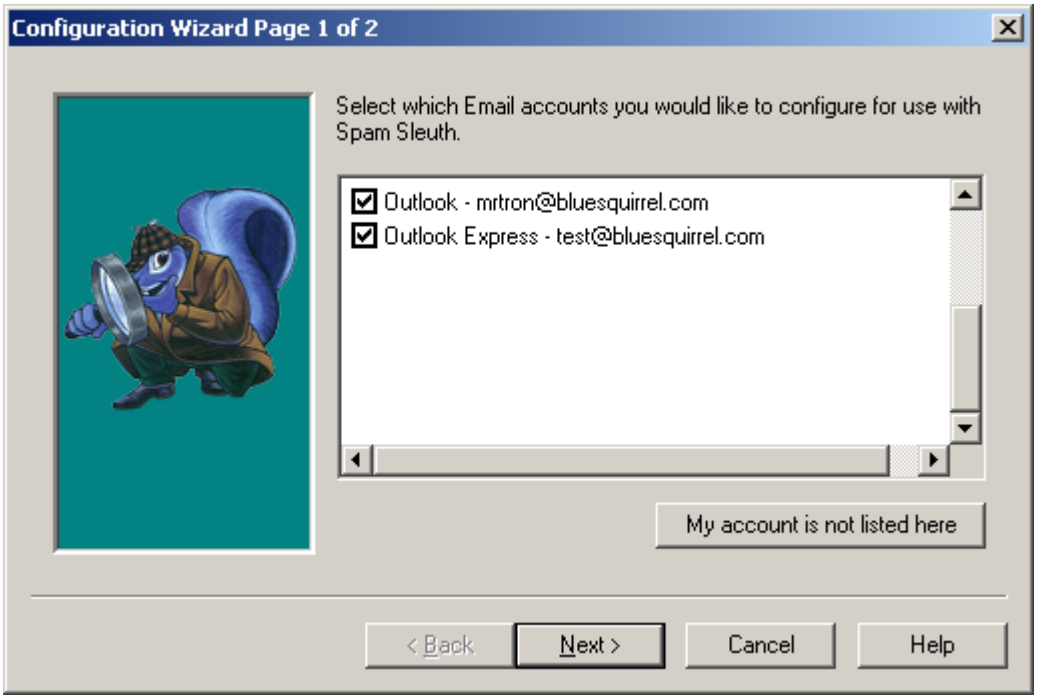
What is '**Polling** Mode'?

In **Polling Mode**, Spam Sleuth will get all of your e-mail from your e-mail server and analyze it. It will determine which messages are spam and will tell the server to delete the spam messages. Spam Sleuth keeps a temporary backup copy of the deleted messages tightly compressed so you can see it in the Mail Jail and UnSpam it if necessary.

In **Polling Mode**, you do not need to make any changes to your e-mail program. But you have to make sure that Spam Sleuth runs before your e-mail program so that it has a chance to get rid of your spam.

Polling Mode is great for cleaning out web accounts that you want to be able to access from anywhere. Spam Sleuth will leave just the good e-mail in the web account.

1.6.2 Configuration Wizard Page 1 of 2

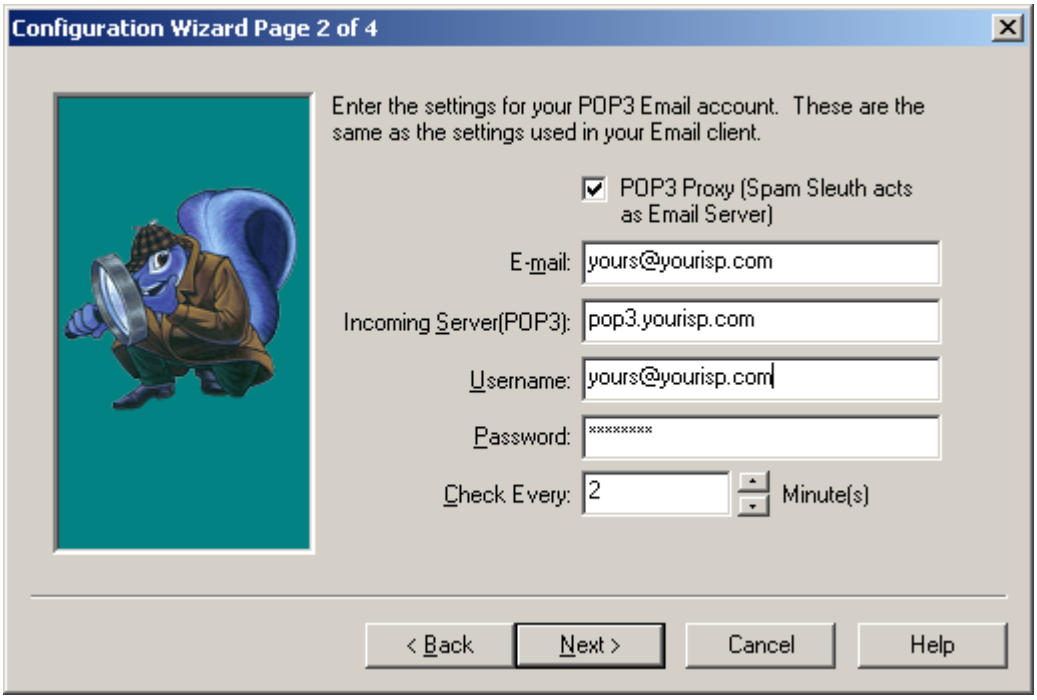


The configuration wizard will run automatically the first time you run Spam Sleuth . To run the configuration wizard later hit CTRL-ALT-W.

Select only the accounts you would like to configure and hit Next.

If the list is blank, or your e-mail program and e-mail address are not shown, it means that Spam Sleuth was unable to find your e-mail account on your computer. If this is the case, choose "My account is not listed here", which will take you to a new wizard page to configure your account manually.

1.6.3 Configuration Wizard Page 2 of 4



POP3 Proxy Mode vs Polling Mode - This is an important setting. If you choose POP3 Proxy Mode, then Spam Sleuth will act as your e-mail server after getting your e-mail and eliminating the spam. If you choose Polling Mode, then Spam Sleuth will analyze all of your e-mail, delete the spam from the server, and leave the good e-mail for your e-mail program to pick up.

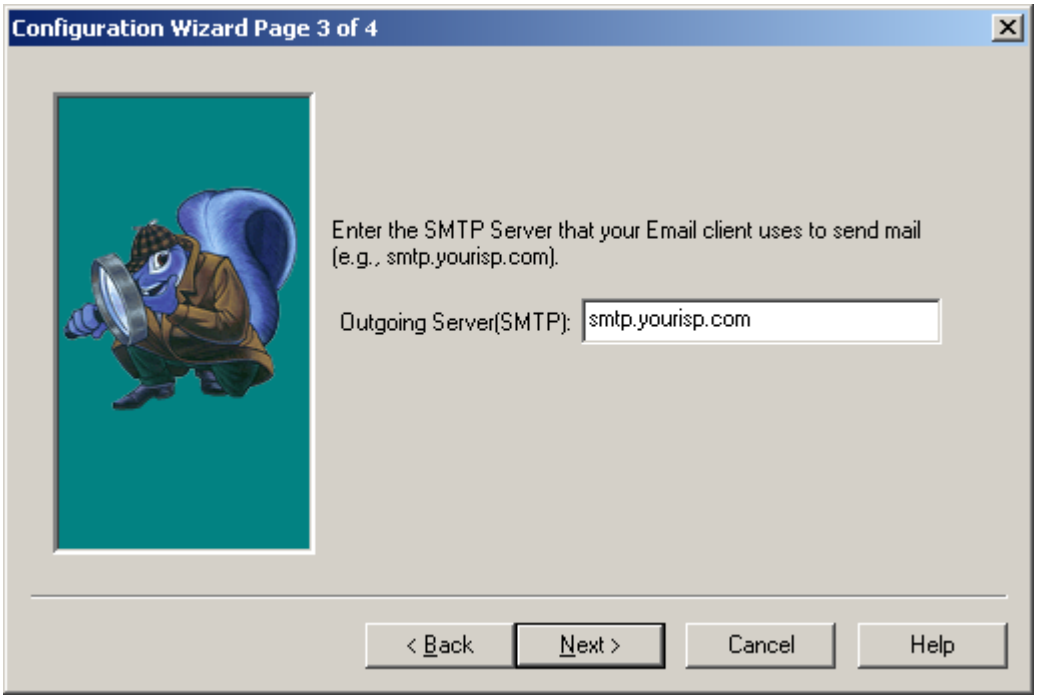
Incoming Server (POP3) - This is the name or IP address of your e-mail server. You can get it from your e-mail program if you don't know it.

Username - This is the username for your e-mail account. It is usually the first part of your e-mail (before the @).

Password - This is the password for your e-mail account. You may leave this blank if you are using POP3 Proxy Mode. If you check for e-mail with your e-mail program, Spam Sleuth will get the password from the e-mail program. If you leave the password blank and you check manually with Spam Sleuth , you will be prompted for the password.

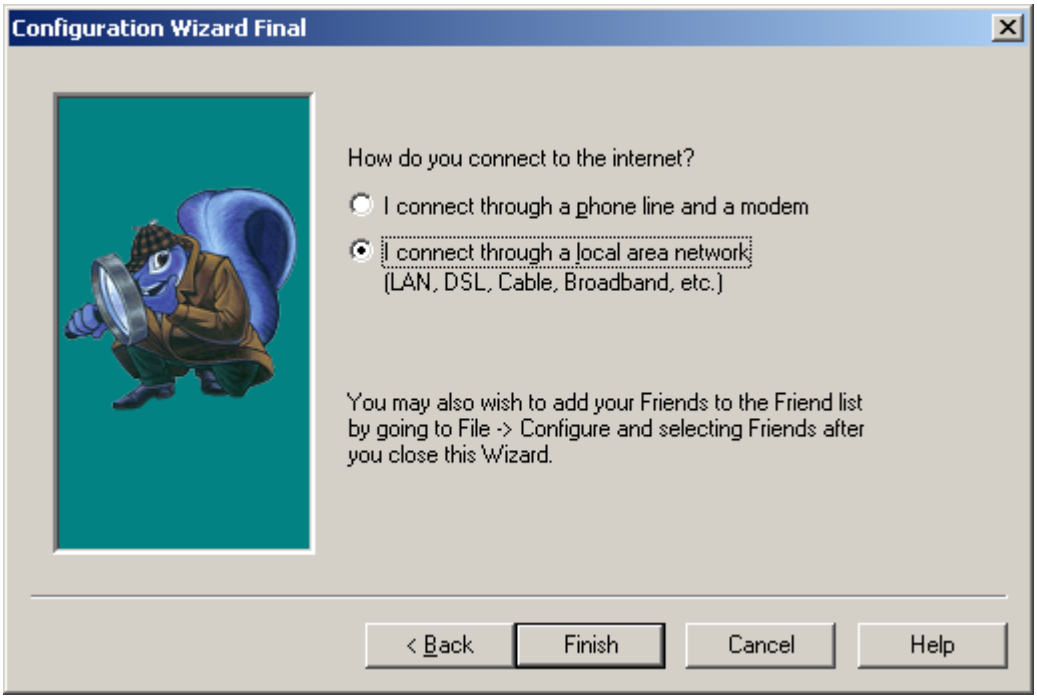
Check Every - This will determine how often Spam Sleuth checks for e-mail. If you are not using **POP3 Proxy Mode**, then make sure Spam Sleuth scans your e-mail before your e-mail program gets your e-mail. If you set it to 0, then it will only check when you check manually, or when your e-mail program checks for e-mail, provided that Last minute check is turned on.

1.6.4 Configuration Wizard Page 3 of 4



Outgoing Server (SMTP) - This is the name or IP address of your outgoing e-mail server. If you don't know this, you can check in your e-mail program.

1.6.5 Configuration Wizard Final



Choose whether you connect through a dial-up connection or through a persistent always-on connection. If you choose dial-up, Spam Sleuth will recognize whether you are online before checking

for e-mail. If you choose 'local area network', Spam Sleuth will check for e-mail on the schedule you set. If it isn't connected, it will just quietly log the error and check again later.

1.7 Configure Accounts

1.7.1 Setup for standard POP3 account (POP3 Proxy Mode)

To set up your account:

In Spam Sleuth
1. Check POP3 Proxy
2. Enter your e-mail address
3. Enter the Incoming POP3 Server (use the one from your e-mail program)
4. Enter your username (usually the first part of your e-mail address)
5. Enter your password
6. Enter the Outgoing Server (SMTP) (use the one from your e-mail program)
7. Set to check every 5 minutes

In your e-mail program
1. Set your Incoming Server (POP3) to 'localhost' (without the quotes) or 127.0.0.1
2. Make sure Spam Sleuth is in your StartUp folder.

1.7.2 Setup for standard POP3 account (Polling Mode)

To set up your account:

In Spam Sleuth
1. Choose Configure...
2. Choose Accounts
3. Hit the Add... button
4. Choose Polling Mode
5. Enter your e-mail address
6. Enter the *Incoming Server (POP3)* (use the one from your e-mail program)
7. Enter the *Outgoing Server (SMTP)* (use the one from your e-mail program)
8. Enter your username (usually the first part of your e-mail address)
9. Enter your password
10. Set to check every 5 minutes
11. Make sure Spam Sleuth checks your e-mail before your e-mail program does

No changes are necessary to your e-mail program. It will continue to get e-mail as it did before. As long as Spam Sleuth analyzes your e-mail first, the account will be cleared of unwanted e-mail before your e-mail program gets your e-mail.

1.7.3 Setup for Hotmail (Polling Mode)

Polling Mode will clean out the spam, but also let you continue to access HotMail from your browser.

To set up your account:

Install Web2POP (http://www.bluesquirrel.com/products/web2pop/)
Make sure Web2POP runs at startup.

In Spam Sleuth
1. Choose Configure...
2. Choose Accounts
3. Hit the Add... button
4. Choose Polling Mode
5. Enter your e-mail address
6. Set the *Incoming Server (POP3)* to the word 'localhost' (without the quotes) or 127.0.0.1.
7. Enter your full hotmail e-mail address for your username. Example: XYZ@hotmail.com
8. Enter your password for your Hotmail account
9. Set to check every 20 minutes

1.7.4 Setup for Hotmail (POP3 Proxy Mode)

POP3 Proxy Mode will let you use Hotmail with your favorite e-mail program.

To set up your account:

Install Web2POP (http://www.bluesquirrel.com/products/web2pop/)
Make sure Web2POP runs at startup.

In Web2POP
1. From the Options tab, make sure "Start Web2Pop when Windows starts" is checked.
2. From the Options tab, set the Listen port to 109.

In Spam Sleuth
1. Choose Configure...
2. Choose Accounts
3. Hit the Add... button
4. Choose POP3 Proxy Mode
5. Enter your e-mail address
6. Set the *Incoming Server (POP3)* to the word 'localhost' (without the quotes) or 127.0.0.1.
7. Enter your full hotmail e-mail address for your username. Example: XYZ@hotmail.com
8. Enter your password for your Hotmail account
9. Set to check every 20 minutes
10. Hit the Advanced... button and set *Port* to 109

1.7.5 Setup for AOL (Polling Mode)

Polling Mode will clean out the spam, but also let you continue to access AOL from the AOL browser.

To set up your account:

Install Web2POP (http://www.bluesquirrel.com/products/web2pop/)
Install AOL support from JMA software (http://www.jmasoftware.com/english/download/addins.html)
Make sure Web2POP runs at startup.

In Spam Sleuth
1. Choose Configure...
2. Choose Accounts
3. Hit the Add... button
4. Choose Polling Mode
5. Enter your e-mail address
6. Set the *Incoming Server (POP3)* to the word 'localhost' (without the quotes) or 127.0.0.1.
7. Set the *Outgoing Server (SMTP)* to aol.com. You'll need to be connected with AOL software.
8. Enter your full AOL e-mail address for your username. Example: XYZ@aol.com
9. Enter your password for your AOL account
10. Set to check every 20 minutes

1.7.6 Setup for AOL (POP3 Proxy Mode)

POP3 Proxy Mode will let you use AOL with your favorite e-mail program.

To set up your account:

Install Web2POP (http://www.bluesquirrel.com/products/web2pop/)
Install AOL support from JMA software (http://www.jmasoftware.com/english/download/addins.html)
Make sure Web2POP runs at startup.

In Web2POP
1. From the Options tab, make sure "Start Web2Pop when Windows starts" is checked.
2. From the Options tab, set the Listen port to 109.

In Spam Sleuth
1. Choose Configure...
2. Choose Accounts
3. Hit the Add... button
4. Choose POP3 Proxy Mode
5. Enter your e-mail address
6. Set the *Incoming Server (POP3)* to the word 'localhost' (without the quotes) or 127.0.0.1.
7. Set the *Outgoing Server (SMTP)* to aol.com. You'll need to be connected with AOL software.
8. Enter your full hotmail e-mail address for your username. Example: XYZ@aol.com
9. Enter your password for your AOL account
10. Set to check every 20 minutes
11. Hit the Advanced... button and set *Port* to 109

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

In Polling-Mode, Spam Sleuth checks your e-mail before your e-mail program. It is up to you to arrange for this to happen. The best way is to set Spam Sleuth to check every minute and your e-mail program to check manually. Spam Sleuth logs into your e-mail account and analyzes all the messages. It stores the spam on your hard drive in a compressed format, and deletes the spam from the server. When your e-mail program checks, the spam will be gone, and you won't have to see it.

In POP3 Proxy Mode, Spam Sleuth gets the e-mail from your e-mail server, eliminates the spam, and then becomes the server for your e-mail program. You must change the settings in your e-mail program to use this mode. In your e-mail program, set your Incoming (POP3) Server to **localhost**, and your login/username to your full e-mail address.

What happens to the spam? It is stored in a safe and highly compressed form, then it is automatically deleted after 30 days. This gives you a chance to recover any messages that may have mistakenly been tagged as spam.

Spam Sleuth is configured by default to remove e-mail attachments that are executables (.exe). Executable attachments are usually viruses. The original e-mail with the attachment will be stored in the Mail Jail. If you want, you can UnSpam the message and get the attachment. Spam Sleuth is also configured by default to remove HTML Script. HTML Script can be dangerous as it can redirect you to other web pages that exploit known security holes in the browser or operating system. You can turn off both of these features in Configure… Use the Attachments tab to turn off attachment removal. Use the HTML Removal tab to turn off the HTML Script removal.

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.

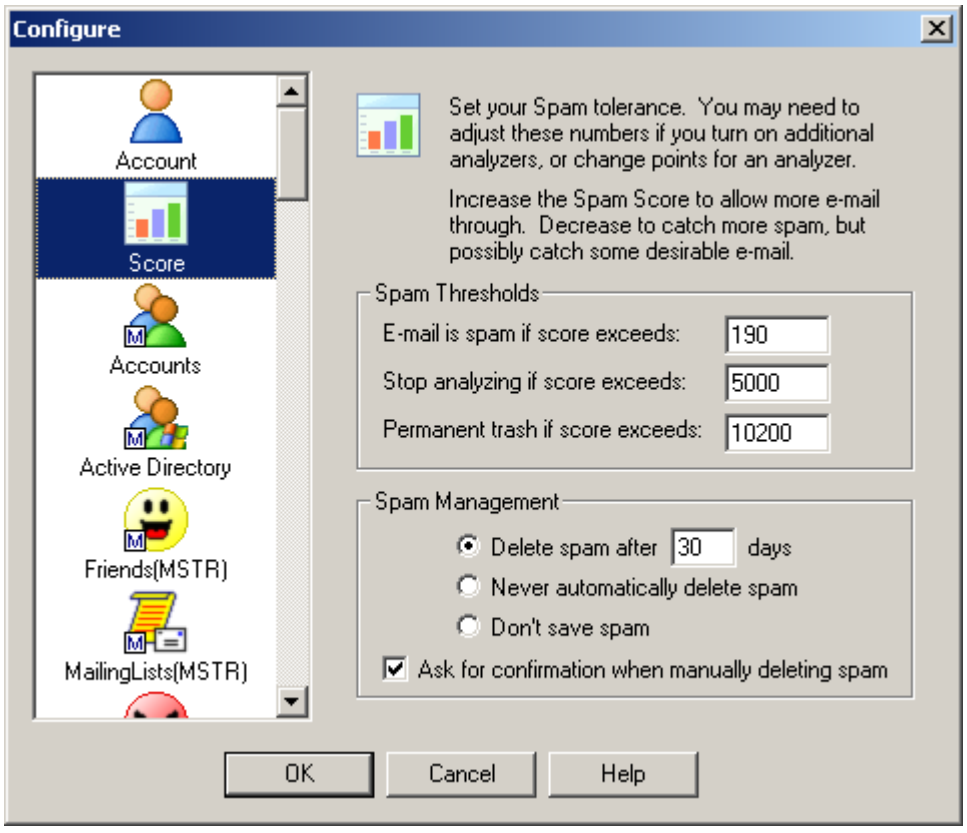
What makes an e-mail spam? Technically, spam is an e-mail that you didn't request, that is commercial in nature and is trying to sell you something or get you to do something. If you signed up for a newsletter, and that newsletter has a sales pitch for the company's product, it isn't technically spam.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

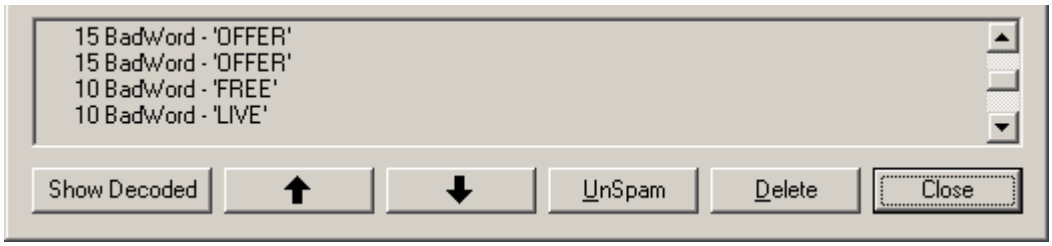
- **Stop analyzing if score exceeds: -** The second Spam Sleuth receives e-mail messages the Analyzers begin adding points. If the points begin to exceed 1,000 Spam Sleuth , the scorekeeper, tells all of the analyzers to stop giving points because it is clear that the e-mail message is spam. These types 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.

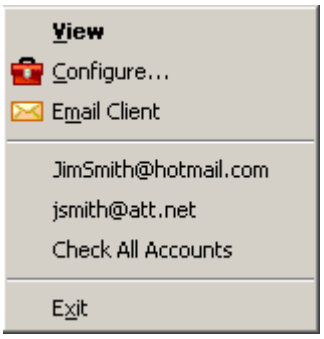
Show Decoded will show the message after decoding characters and Base64 encoded text. It will not decode attachments.

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

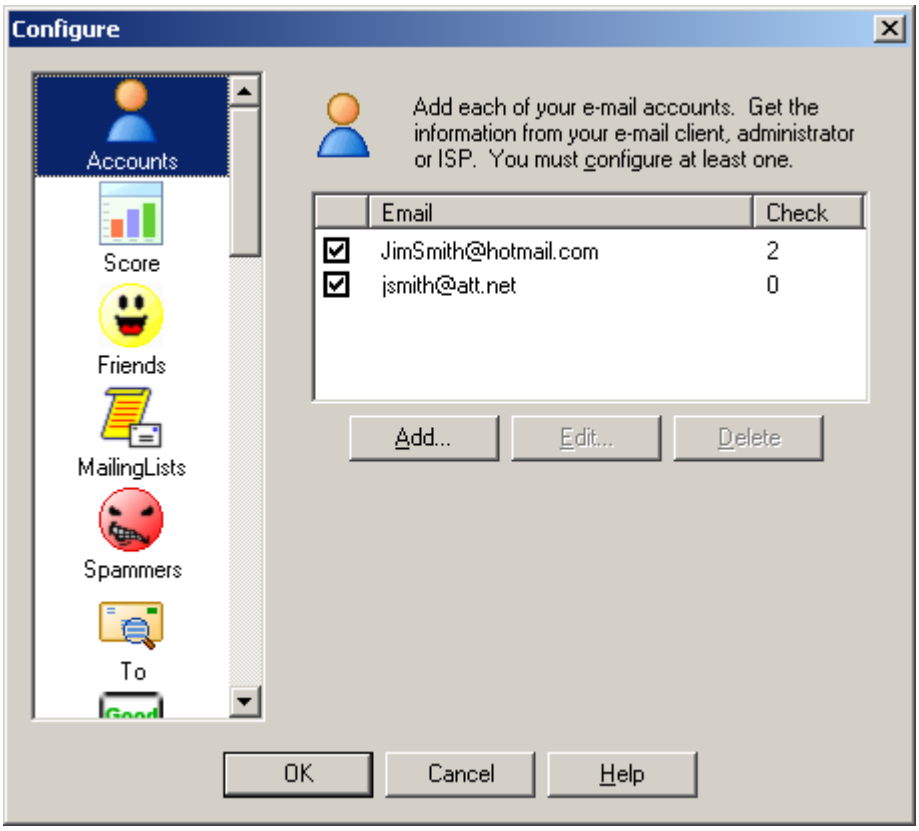
Most of the time the only thing you'll see is a small icon that sits in your Windows system tray . Once configured, Spam Sleuth ™ monitors your e-mail accounts and removes spam before you or your e-mail program sees it.

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 Account Configuration

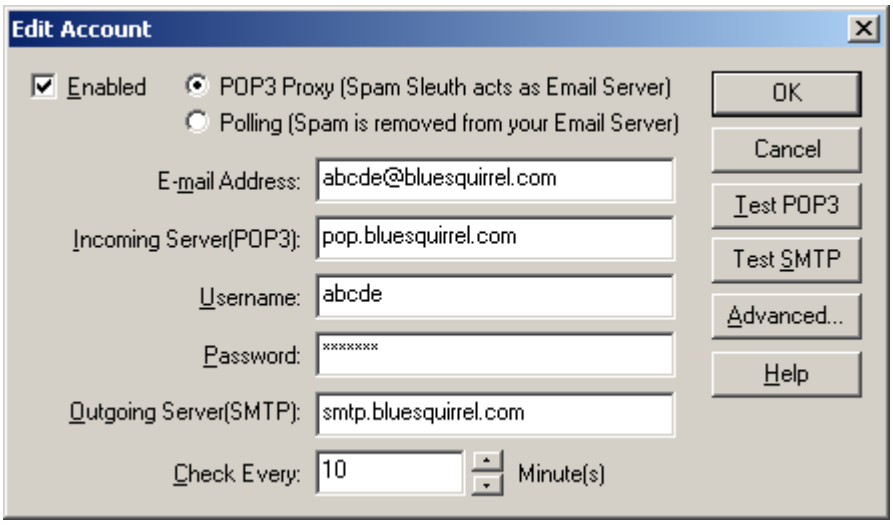


To add a new e-mail account, just hit the Add… button. You will be taken to the Edit Account dialog. You can add up to 25 accounts.

To edit an exisiting account, highlight the account and hit the Edit... button. You will be taken to the Edit Account dialog.

To delete and existing account, highlight the account and hit the Delete button.

3.1.1 Edit Account



Enter the same information that you would enter into your e-mail program configuration. If you do not know what to enter, check the settings in your e-mail program, or contact your ISP.

POP3 Proxy vs. Polling Mode – This very important setting determines whether the program works in *Polling-Mode* or *POP3 Proxy Mode*. In *Polling-Mode*, Spam Sleuth removes spam from your server and leaves the good e-mail for your e-mail program to pick up. In *POP3 Proxy Mode*, Spam Sleuth will remove all the e-mail from your server and then becomes the POP3 server for your e-mail. *POP3 Proxy Mode* requires that you change the settings in your e-mail program to these settings: POP3 Server: localhost Username: <full e-mail address>

E-mail – Your e-mail address for this account.

Incoming Server (POP3) – The server name or IP address of your POP3 server.

Username – Usually this is the first part of your e-mail address (before the @ sign).

Password – The password you use to get your e-mail. You may leave this blank if you have POP3 Proxy turned on. Spam Sleuth will use the password provided by your e-mail program. If you check for e-mail manually with Spam Sleuth and the password is blank, you will be prompted for the password.

Outgoing Server (SMTP) – The server name or IP address of your SMTP server.

Check Every – This setting determines how often Spam Sleuth ™ checks for spam.

Test POP3 – This button will show you the communication between Spam Sleuth and your POP3 Server. It logs on and quits. If you don't see any results, or you see –ERR, there is probably something wrong with Incoming Server, Username, or Password.

Test SMTP – This button will show you the communication between Spam Sleuth and your SMTP server. It starts to send an e-mail and then quits. If you don't see any results, or you see errors, there is probably something wrong with Outgoing Server, or your E-mail address.

Advanced – This button takes you to some additional settings including the port to use for the POP3 Proxy, and SMTP authentication settings if your ISP requires them.

3.1.1.1 Incoming Server (POP3)

This is the name or IP address of your POP3 server. This is the computer serves your e-mail to your e-mail program.

Some examples:
For Netcom users: pop.ix.netcom.com
For Earthlink users: pop.earthlink.net

If you set your *Incoming Server (POP3)* to **localhost**, it means that the program being configured is getting e-mail from your own machine. This can happen for two reasons:

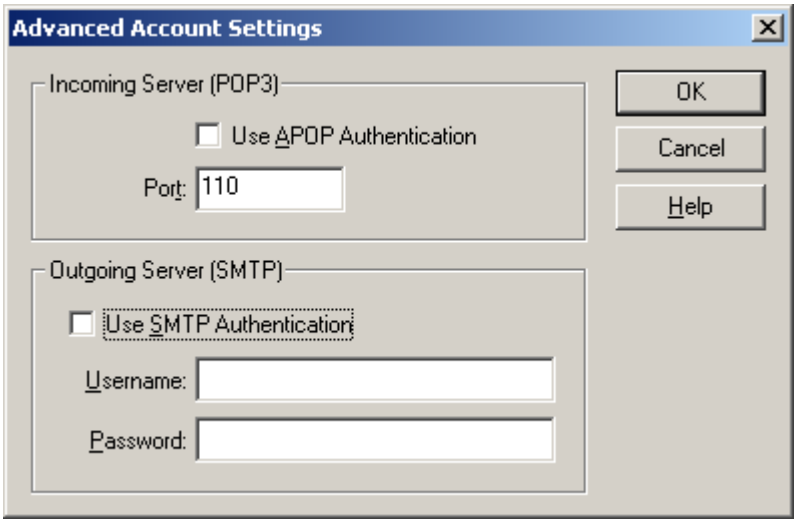
1. Your e-mail program is getting e-mail from Spam Sleuth in POP3 Proxy Mode
2. Spam Sleuth is getting e-mail from a gateway program like Web2POP

3.1.1.2 Outgoing Server (SMTP)

This is the name or IP address of your SMTP server. This is the computer that accepts e-mail sent from your e-mail program.

Some examples:
For Netcom users: smtp.ix.netcom.com
For Earthlink users: smtp.earthlink.net

3.1.1.3 Edit Account - Advanced



Use APOP Authentication – Some POP3 servers require encrypted Authenticated POP. If your ISP's server requires APOP, then check this setting.

Port – The default port for POP3 is port 110. This is the port Spam Sleuth will use to go get e-mail. Do not confuse this port with the Listen port which is configured in Miscellaneous. Only change this setting if you have a specific reason that Spam Sleuth needs to communicate with an e-mail server on a different port.

Use SMTP Authentication - If your ISP requires authentication to send mail (not common), then check this box. If the username/password is the same as your POP3, then you can leave the SMTP Username/Password blank, and the program will use your POP3 Username/Password.

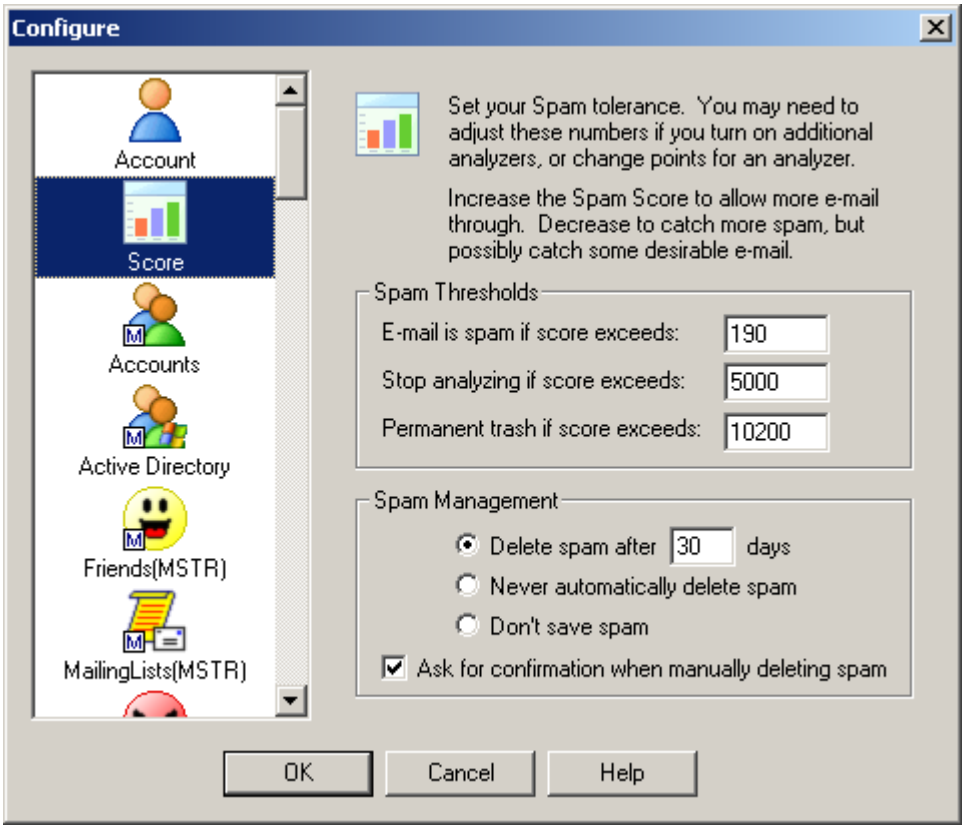
Outgoing Server (SMTP) Username/Password: - If your ISP requires a username and password to send e-mail (most don't) then you'll need to set that information here.

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

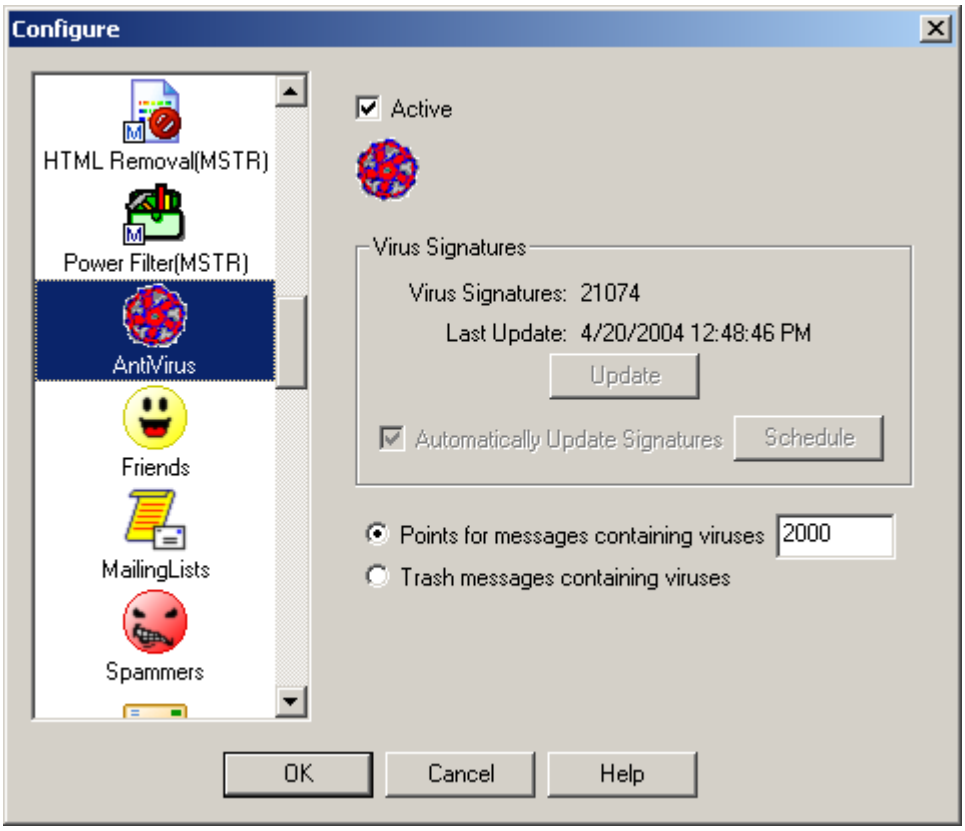
The spam will keep on coming, but you probably don't want to keep it forever. Spam Sleuth does compress the messages so they take less room on your computer. Spam Sleuth will permanently delete spam after so many days. You decide how long to keep it in storage. We've set the default to 30 days, but you 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*.

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

3.2.2 AntiVirus



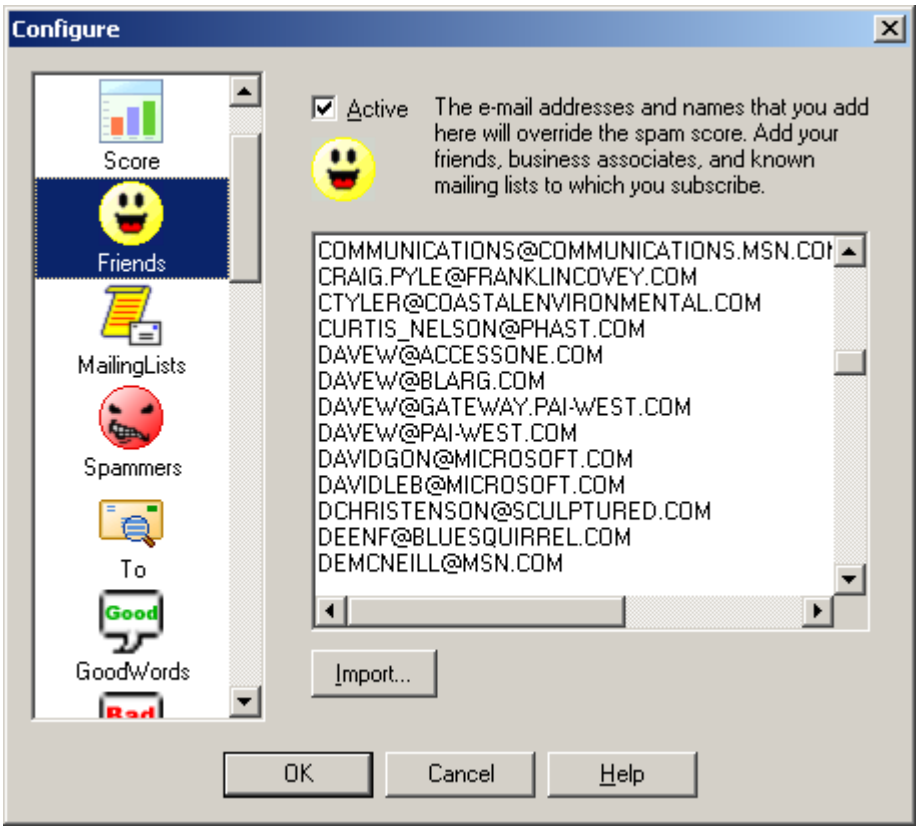
The Anti-Virus analyzer scans incoming message attachments for viruses. If viruses are found the message is assigned points or the message is eliminated.

Messages containing viruses will appear with a virus icon next to them.

3.2.3 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.

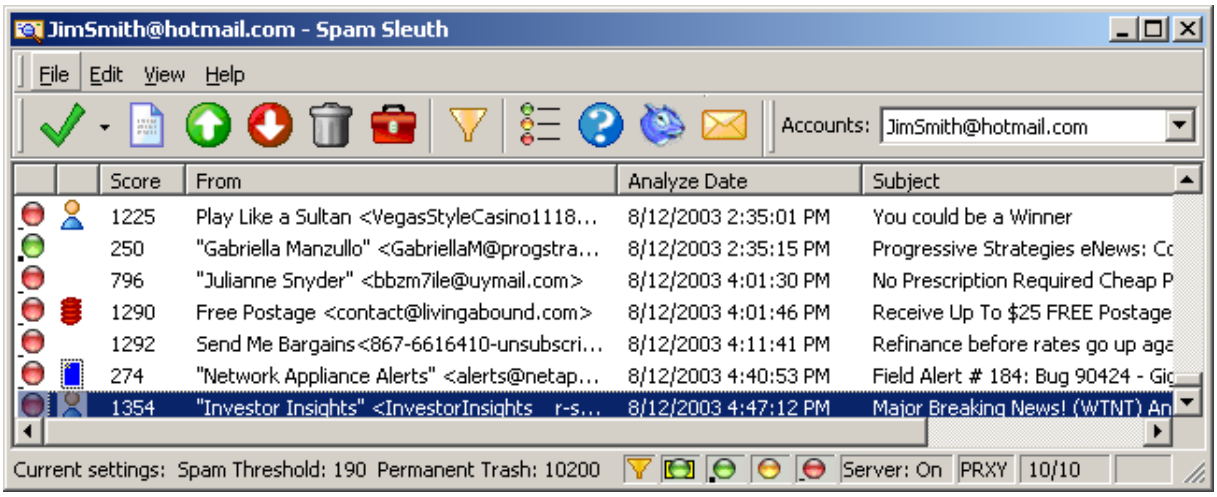


The Friends dialog lets you add e-mail addresses for your family, friends, co-workers and mailing lists. If someone in this list sends you an e-mail, Spam Sleuth will route the message directly to your e-mail program. Spam Sleuth will still strip off dangerous attachments, but you will get the e-mail. 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.

3.2.4 Mailing Lists

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



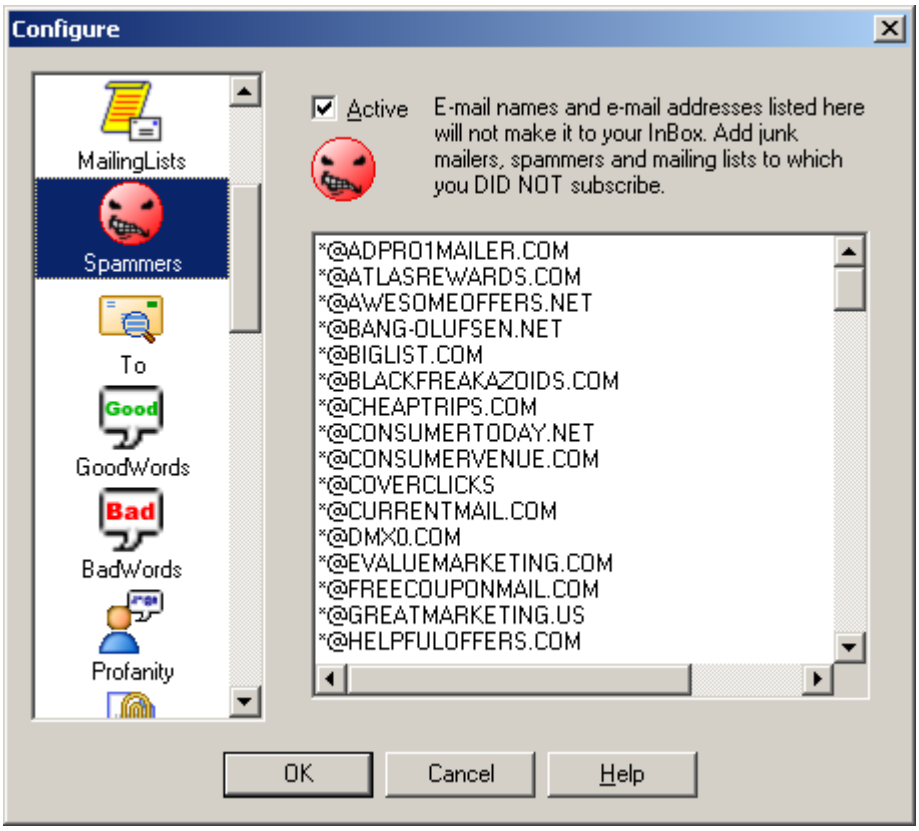
Mailing Lists lets you by-pass the analysis for the mailing lists for which you have subscribed. It is very similar to Friends, but will also check if the To: matches the mailing list name.

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.

3.2.5 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.

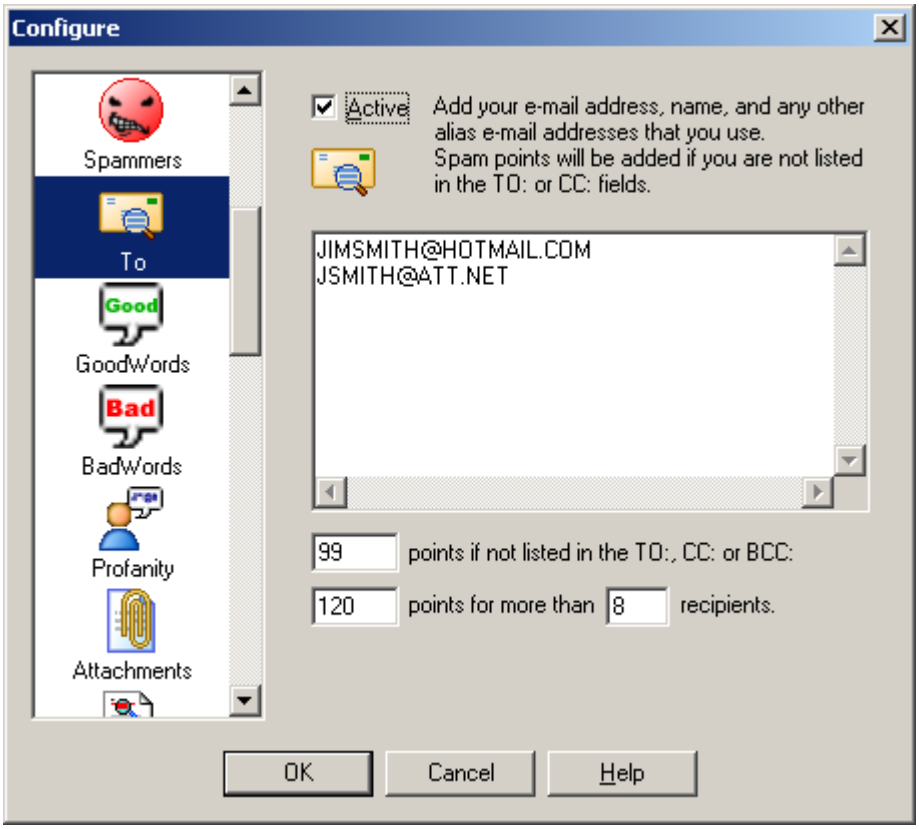
To block e-mails that use various subdomains, like out@mailout.blastmail.com, or out@outgoing.blastmail.com, etc., then you can add *BLASTMAIL.COM to the Spammers list to catch all of them.

3.2.6 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.

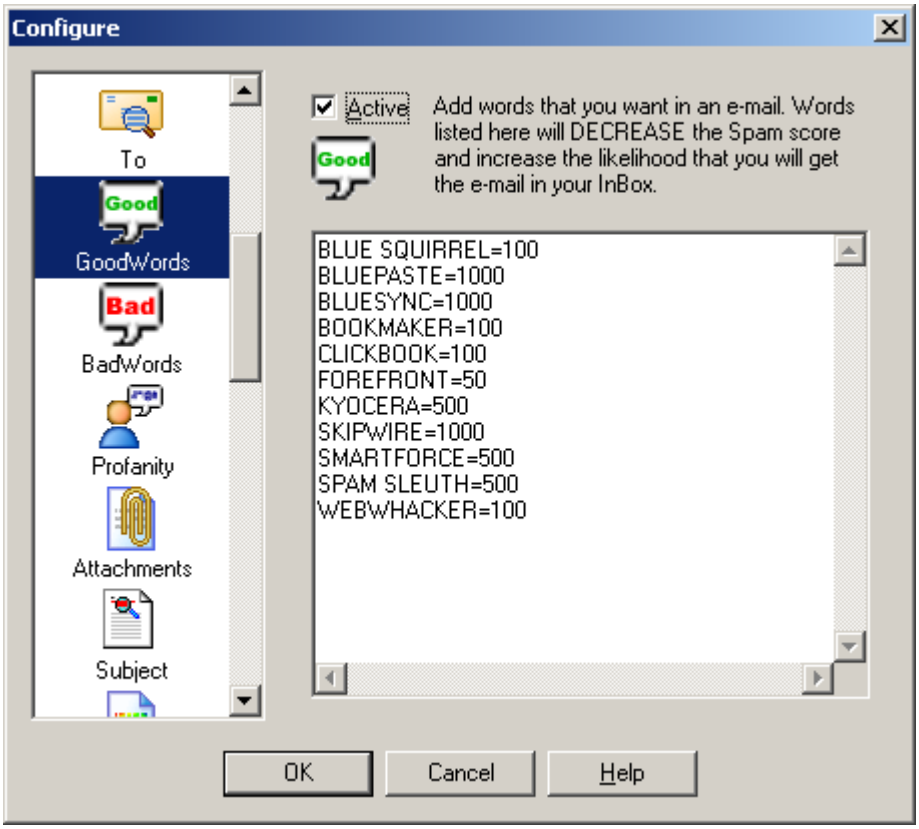
You may be wondering how the message could get to you without your e-mail address being listed. The server that sent it specified that it was for you, but the text of the message which you see (To: joe@xyz.com) can be anything and does not have to list your name. Often times it is more efficient for 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.

3.2.7 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.



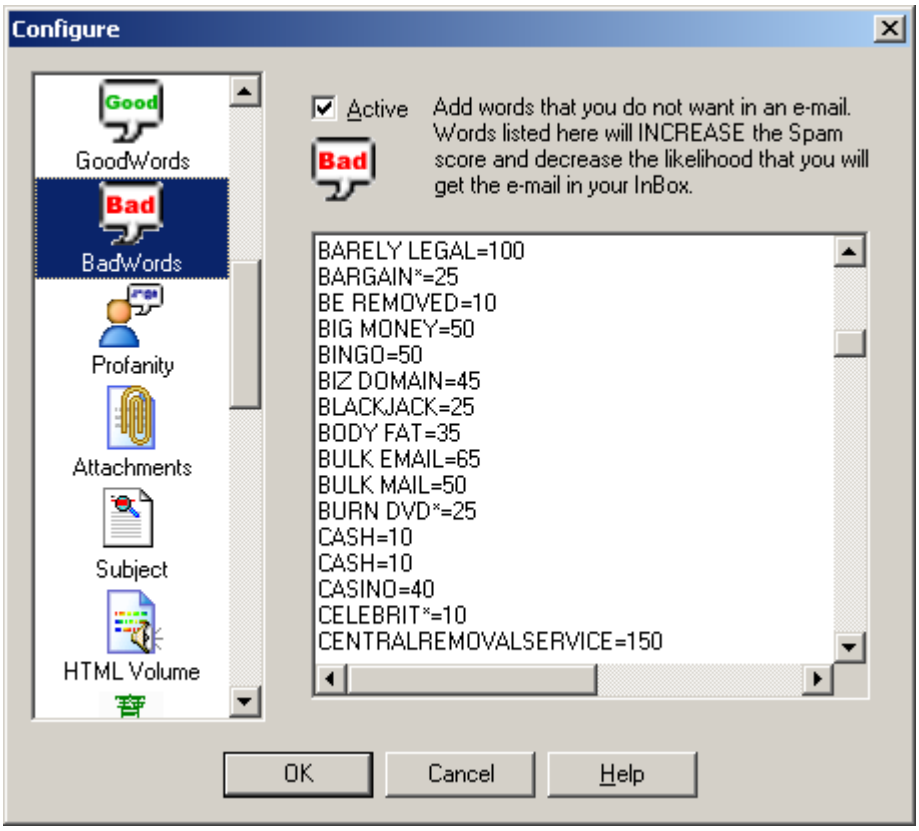
GoodWords let you catch e-mails that may interest you. At Blue Squirrel we have a number of products. If our product names are in the e-mail, we probably want the e-mail even if it has some spam characteristics. The GoodWords will be different for everybody. You might put in sports, or hobbies that interest 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"

3.2.8 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. Spam Sleuth will honor your point changes, and deletions even when the automatic updater updates the master list of BadWords.



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.

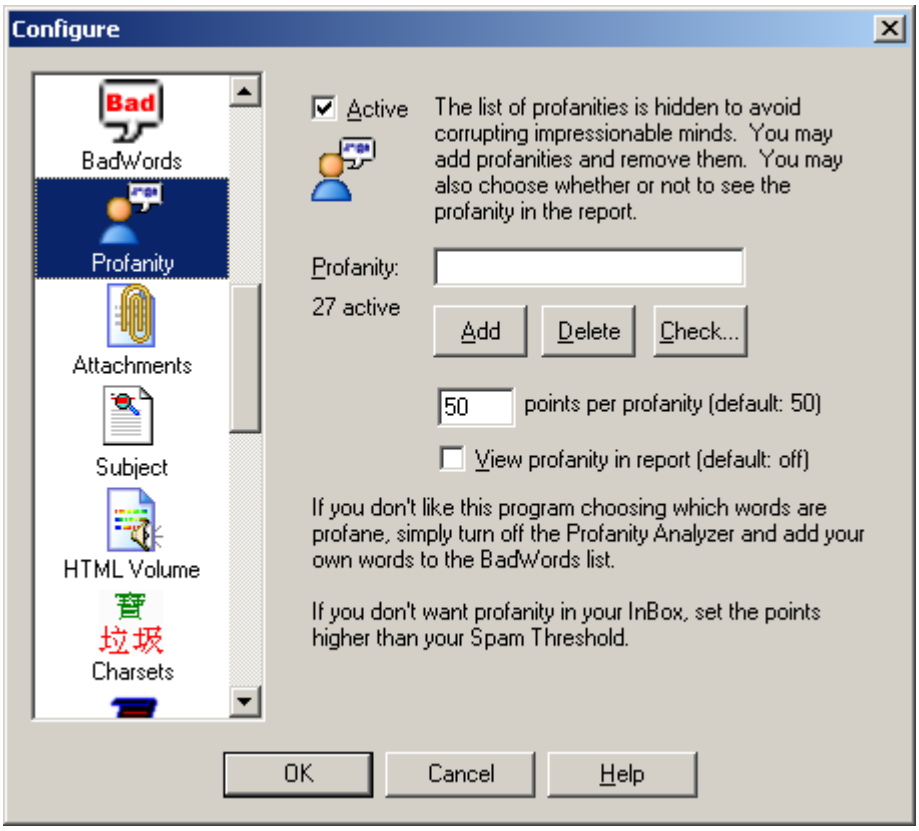
BadWords will search the entire message, including the header (with the subject).

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"

3.2.9 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.

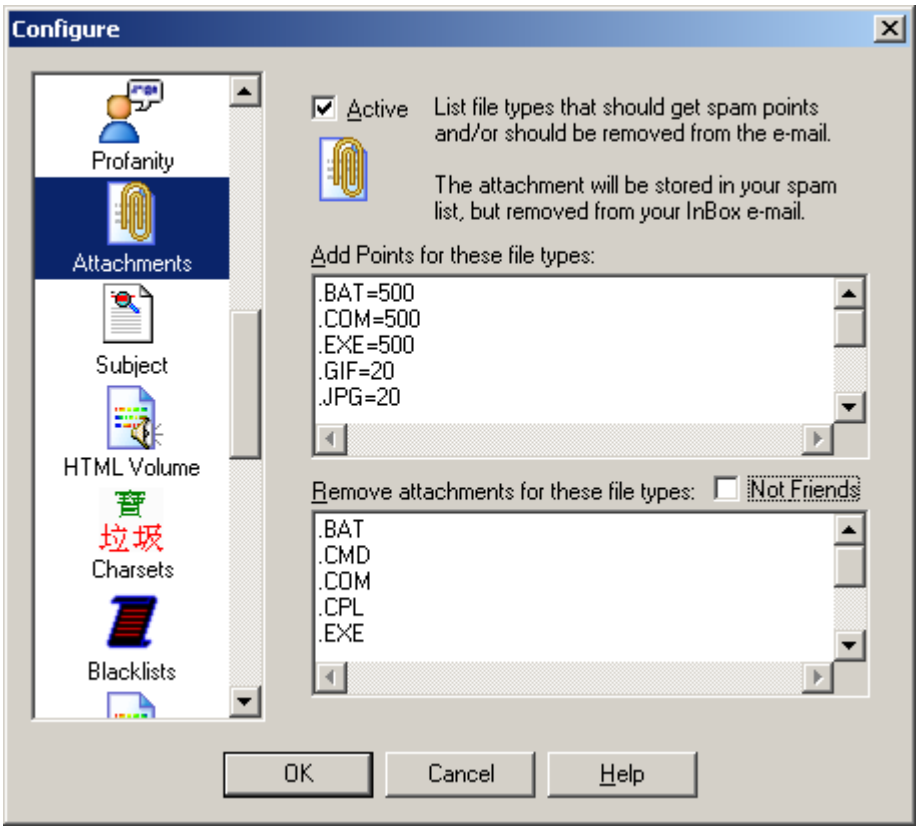
You can add profanities to the list, and you can delete them from the list if you know what they are.

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.

3.2.10 Attachments

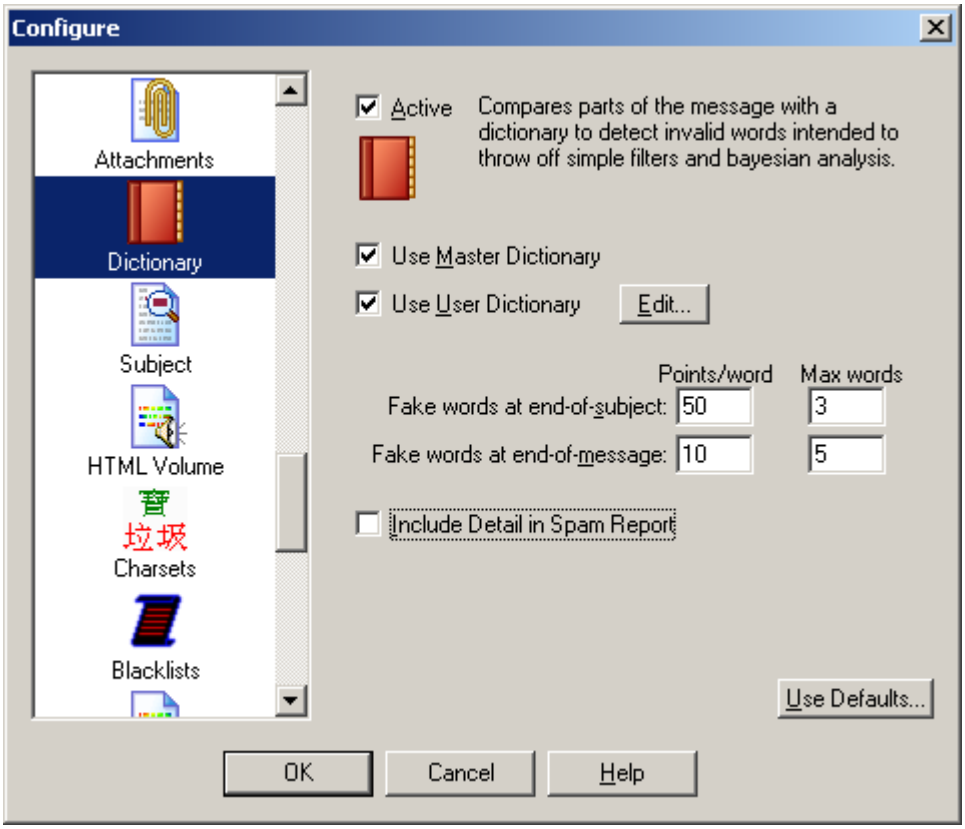
Did you know that all e-mail viruses are spread by sending attachments that can be executed? The **Attachments Analyzer** removes dangerous attachments, such as .exe files. Don't worry it stores the entire e-mail along with the attachment in the Mail Jail if you need it back. Be very careful. Most e-mail 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.

3.2.11 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.

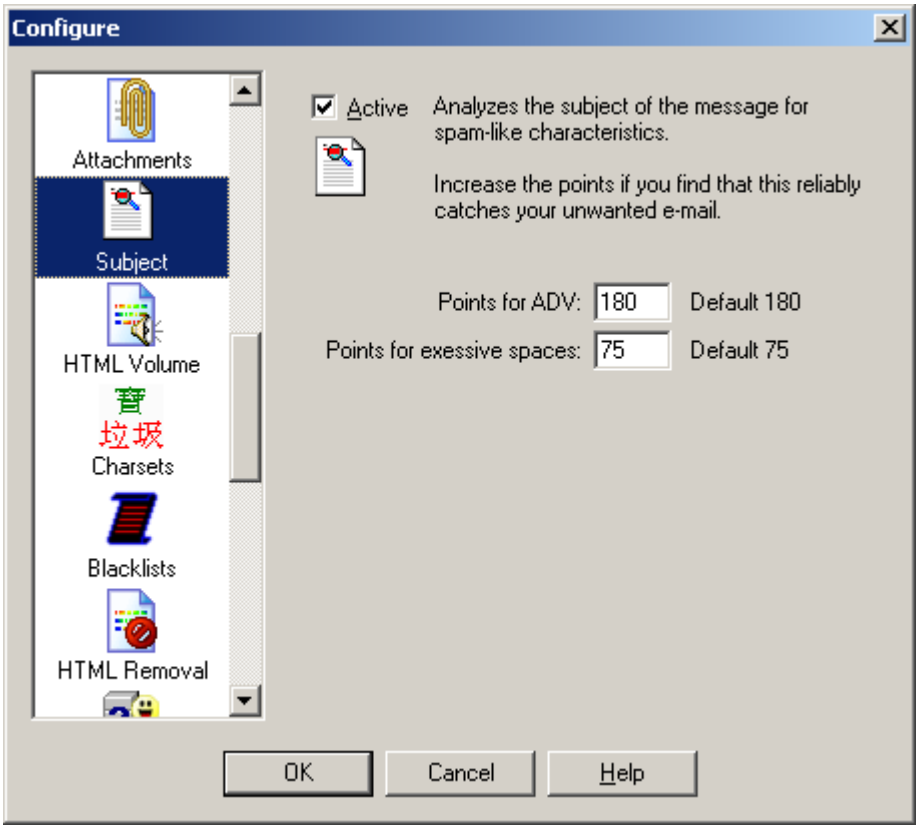
Fake words at the end of message - By default, the last two words of the message are analyzed and 10 points per non-word is added to the total score.

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.

3.2.12 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.

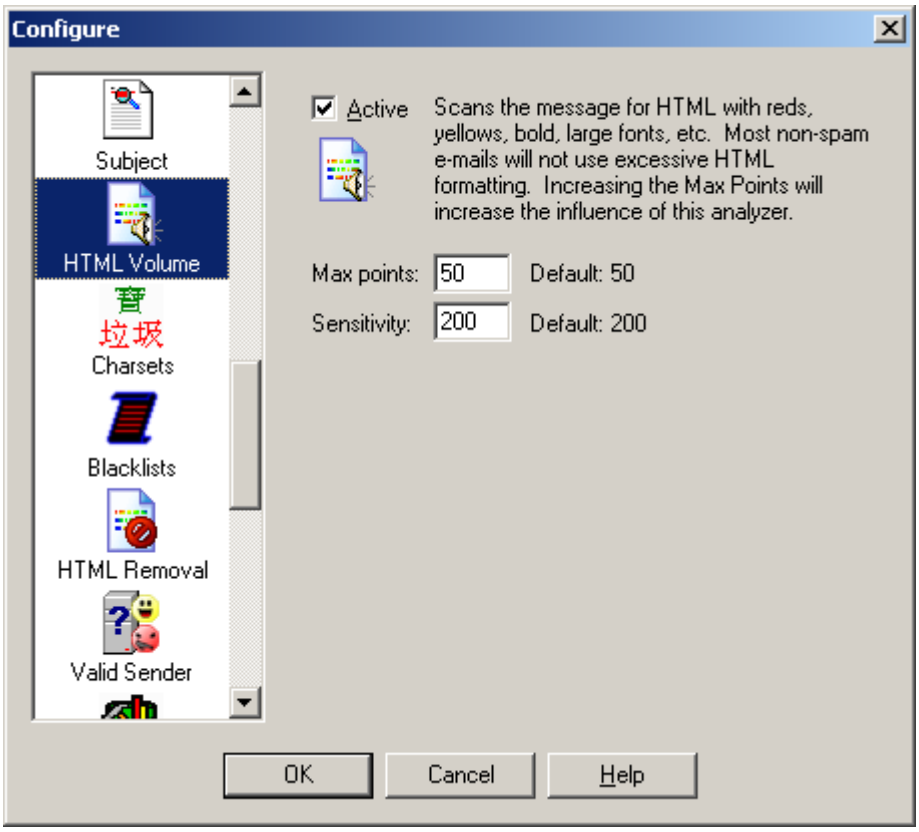
Points for no subject line - Set the points that will be assigned when a message has no subject line in the header. This is rare, but does happen with some spam.

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.

3.2.13 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.

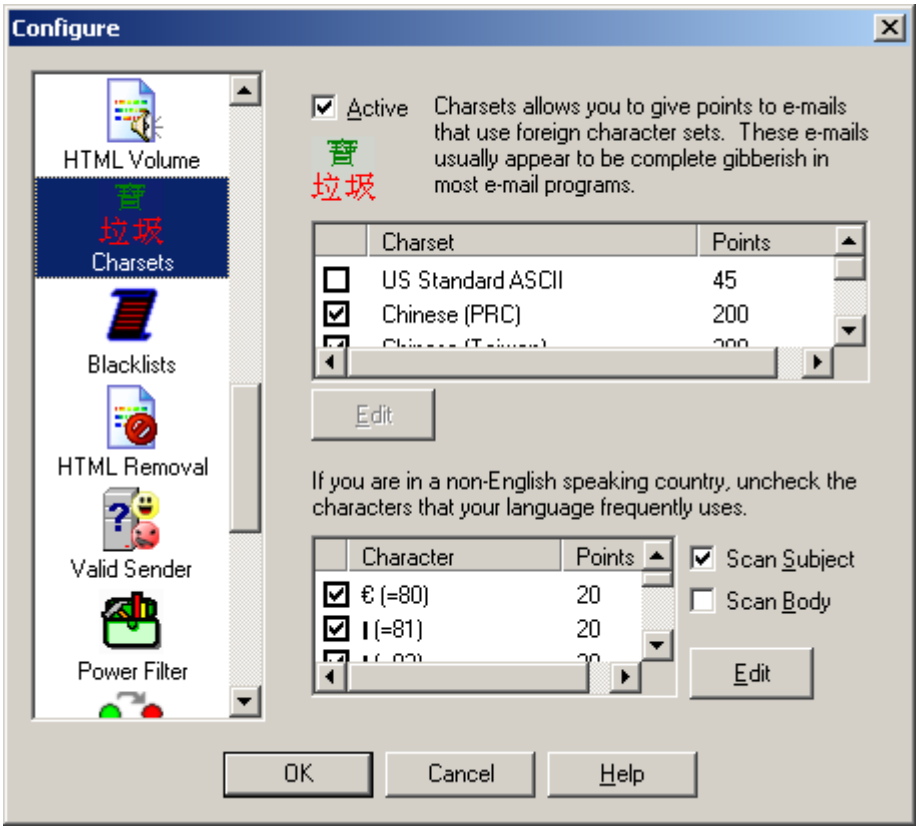
If you have "loud" friends that e-mail you in big bold, red letters, then you may want to either turn this analyzer off, decrease its influence on the total score by lowering the Max points, or pick new friends.

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.

3.2.14 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 - ÞÕýÔÚÂüÑÓ¡¢º þ±±Ò»Ãû¹¤ÈË¾ÍÕâÑù.

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.

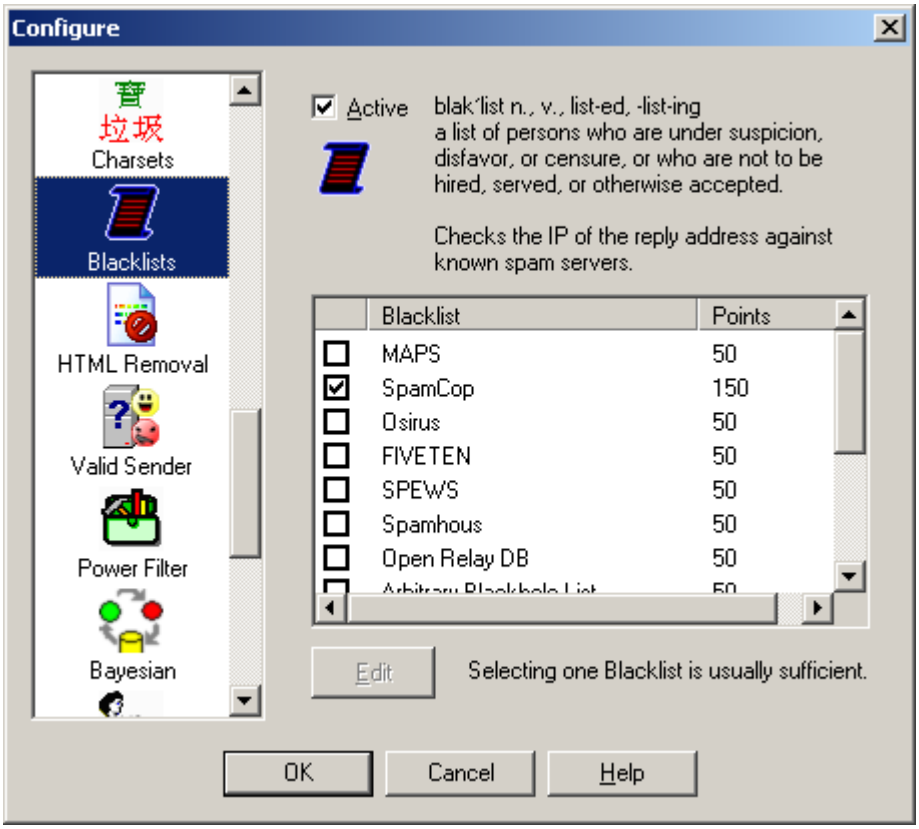
Spam Sleuth can also check for any high-bit characters. These are characters that are above the 127 in the ASCII set. All high-bit characters are selected by default. They are usually only used by non-English speaking countries. If you are in Germany, we recommend that you uncheck characters in your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

3.2.15 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).

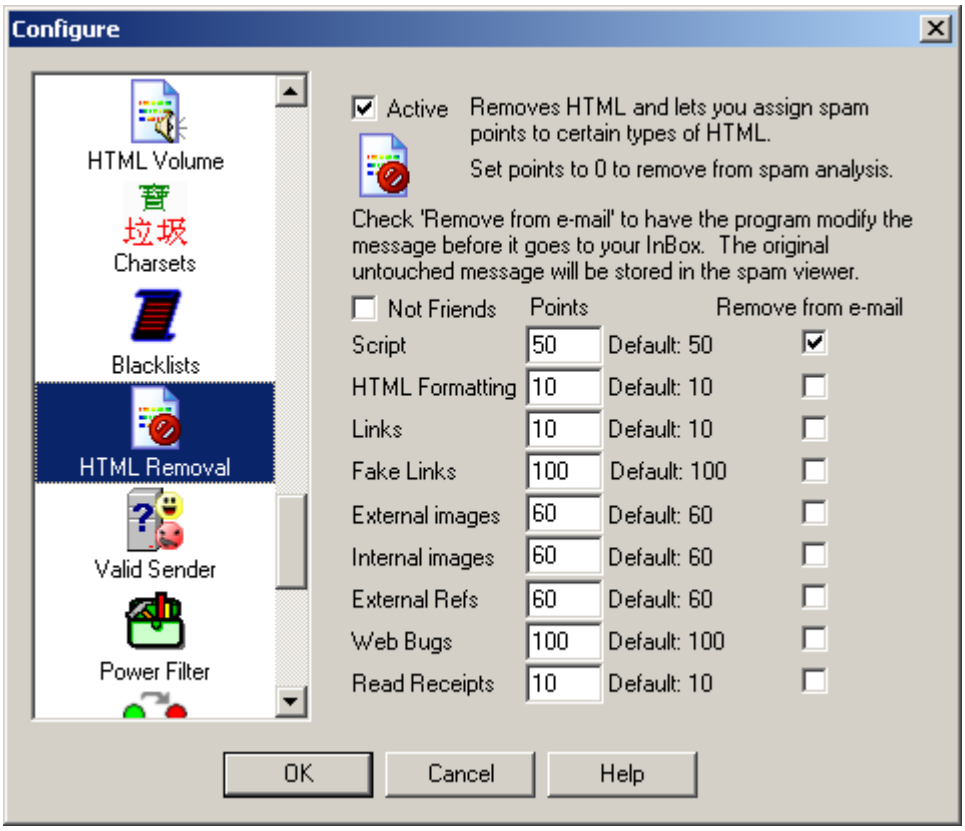
You can edit the number of points assigned when a blacklist reports that the IP is a known spammer.

3.2.16 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, you 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 you 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.

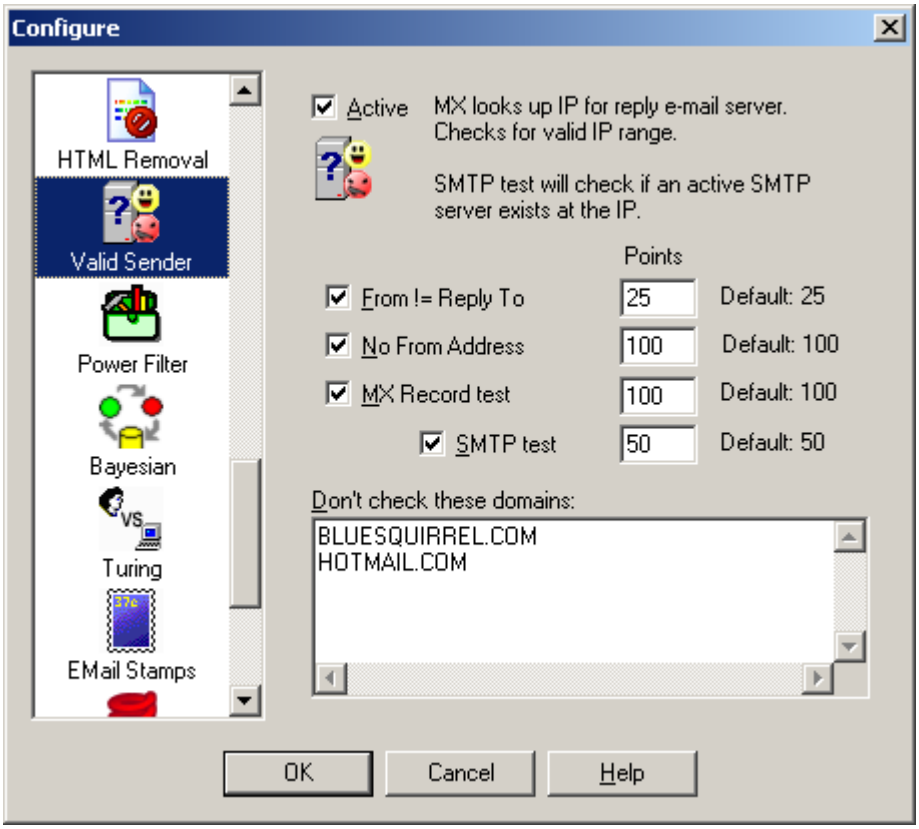
Read Receipts - This is an e-mail header tag that tells some e-mail clients to notify the sender that you've read their message. Some e-mail programs ignore it, some let you decide whether to notify the sender, and some just notify the sender automatically. Spammers don't use these very often, but you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

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

3.2.17 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 Sender 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 Sender 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 Sender 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.

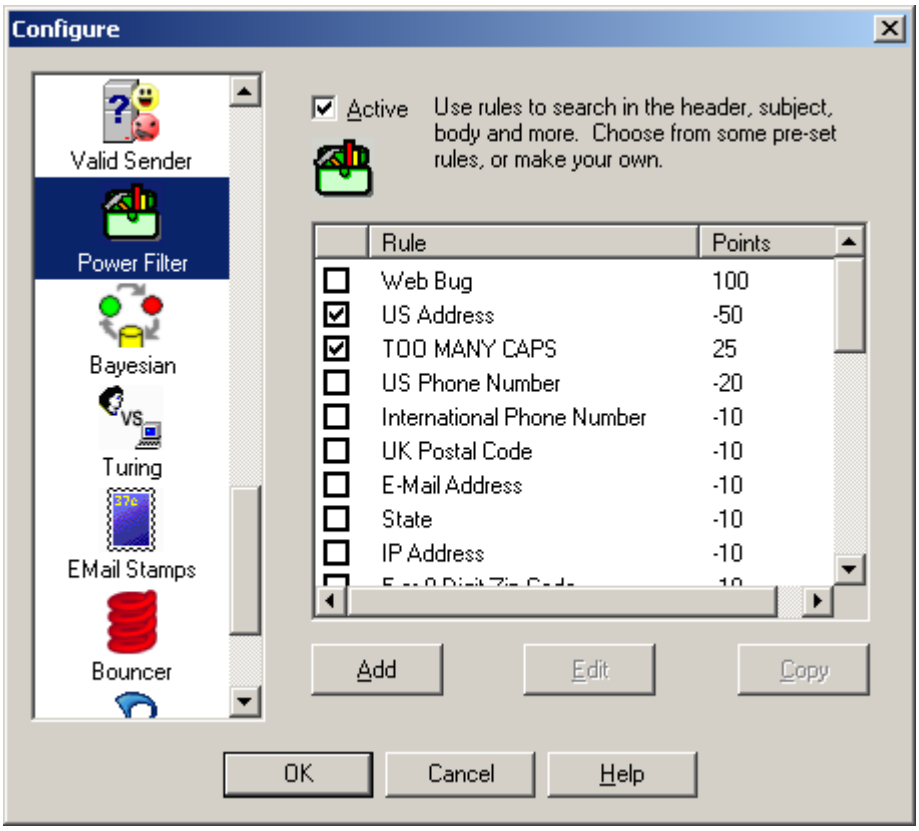
An MX Record test takes a few seconds. Your computer will look up the e-mail address and make sure there is an IP address available to send a reply if you wanted to send one. In the physical world this would be equivalent of looking up the return address on an envelope in the phone book.

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.

3.2.18 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.

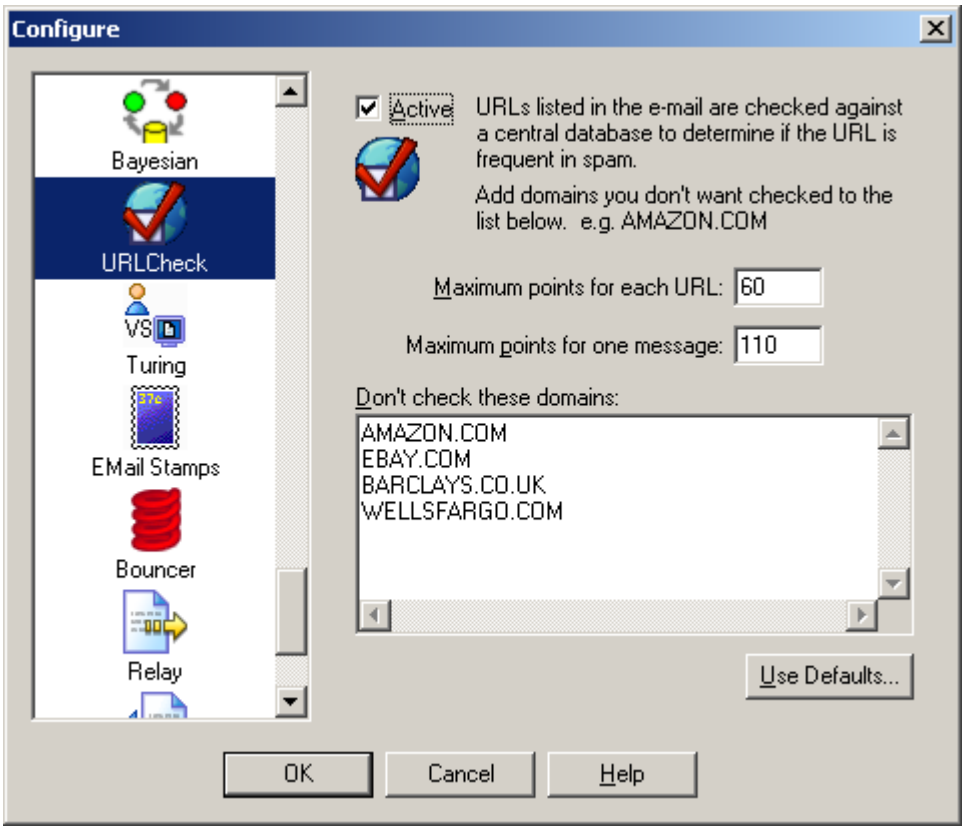
The pre-defined filters use a powerful regular expression syntax that allows complex pattern matching. The details of the regular expression syntax are listed in Appendix A. Be careful, as some complex regular expressions can take a long time to match in a large e-mail message.

3.2.19 URLCheck

Some spam messages are very difficult to detect because they have just and image and a link. By sharing information about the URLs in these messages, it is possible to detect these messages by the frequency that those URLs appear in messages.

Warning: *URLCheck sends information about the links found in e-mail messages. It will not send any*

information for messages with a score less than 0, so URLs from messages from Friends will not be analyzed.



URLCheck will send the domain and first directory to a centralized server. The server returns a probability that the URL is in a spam message based on how many times the URL has been seen in a period of time.

Setting the *Maximum points for each URL* will determine how many points will be assigned to the message if the centralized server reports 100 as the probability of a bad URL. Fewer points will be assigned if the centralized server returns a smaller probability.

Setting the *Maximum points for one message* will determine the overall influence of this analyzer. If there are many URLs that are really bad in the message, the maximum will be reached, but no more that this number of points will be assigned. All URLs will be checked until the maximum points is reached.

If you do not want the URL information to be sent out, turn off this analyzer by unchecking *Active*.

If the message was sent from someone in your Friends list, or in your Mailing Lists, it will not be analyzed by this analyzer.

When a domain is known to be good, the central server will return a 0 probability that the URL is bad. The database is not perfect, and may return a high probability that the URL is spam only because a perfectly legitimate company sends out large amounts of e-mail with their URL in it.

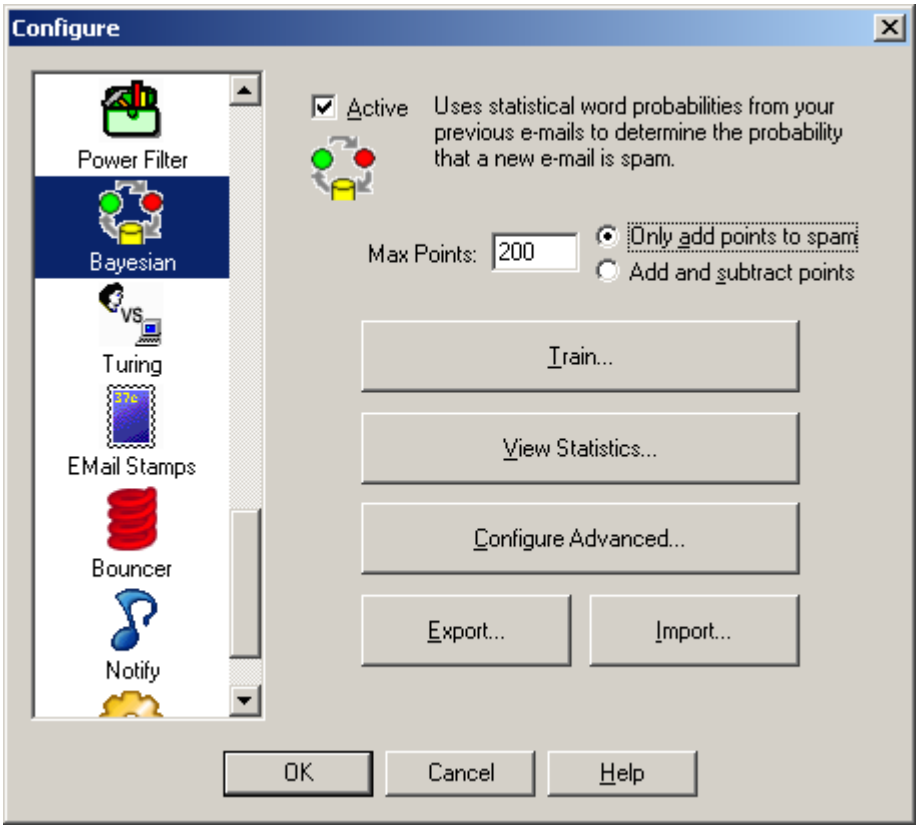
If you know that a particular domain is good, add it to your own personal list of good domains. The good domain list is never sent to our server. The list simply prevents the analyzer from making the check if the URL in the message is from one of the domains in your list.

The domains that you add must be in a very specific format. Use only the first two levels, like **AMAZON.COM**, and NOT **WWW.AMAZON.COM**. If the second level of the domain is **CO**, **COM**, **NET**, or **EDU** as in **CO.UK**, then add one more level like **BARCLAYS.CO.UK**. If you do not follow these rules, the URL will be sent and points may be assigned.

3.2.20 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.

3.2.20.1 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.

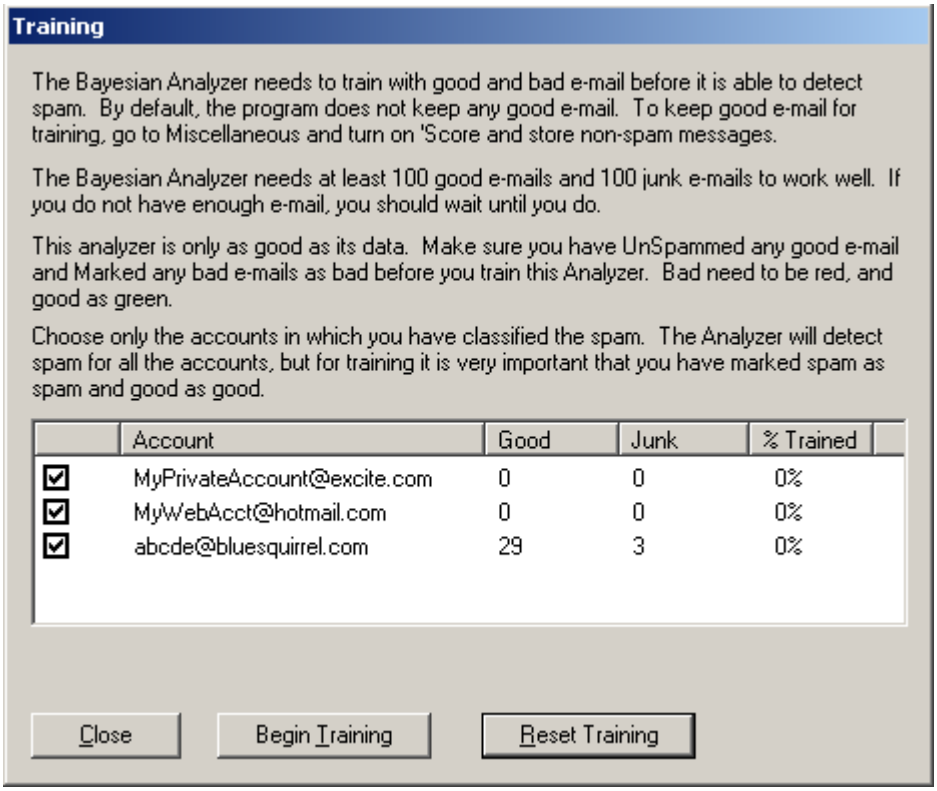
Every e-mail is broken down into words. For every word, the analyzer figures out the probability of a message being spam if that word appears in the text of the e-mail. This information is built during training. In order for the Bayesian Analyzer to figure out these probabilities, it must know in advance 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.

3.2.20.2 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'

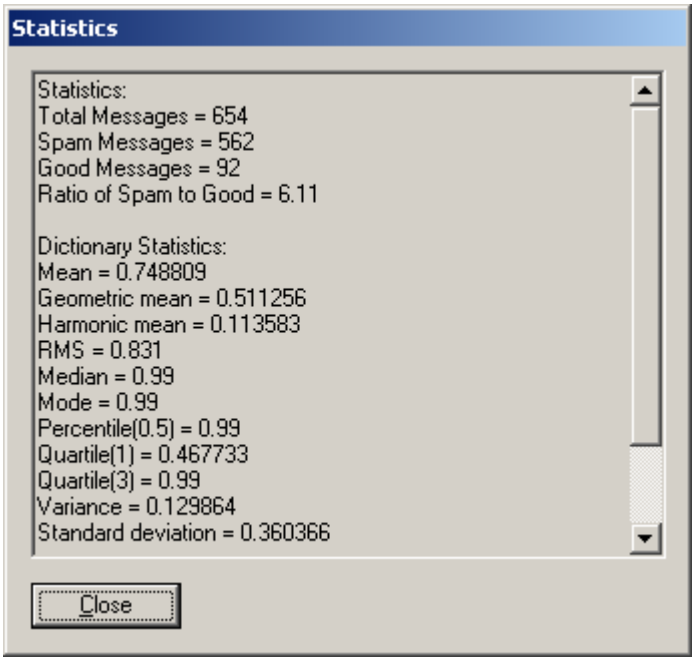
Choose only the accounts for which you have categorized the e-mail as spam and good. The spam messages should have a red dot next to them, and the good messages should have a green dot next to them. Spam Sleuth will do most of the work automatically, but you need to correct any mistakes it may have made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

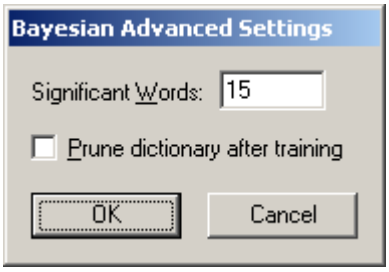
The **% Trained** will always show 0% when you enter. The % trained will change as it trains.

3.2.20.3 View Statistics



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

3.2.20.4 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.

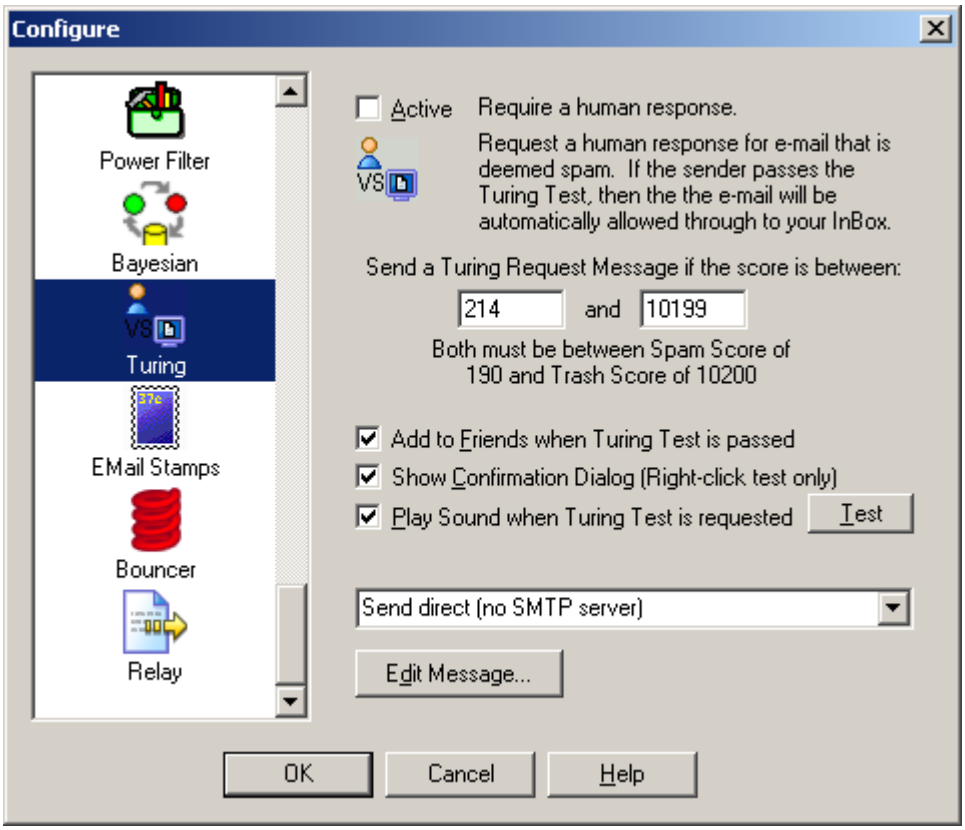
Prune dictionary after training - determines whether the dictionary will be purged of non-significant words before saving. The non-significant words are words that have not appeared enough times in your spam or good e-mails to be considered in the calculations. This is not selected by default because 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.

3.2.21 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.

Play Sound when Turing Test Passed - Plays a sound when someone has passed the Turing Test and an e-mail has been released to your InBox. To change the sound, replace the `TuringPass.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.

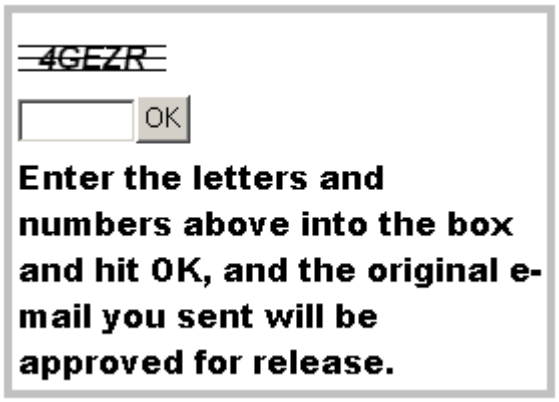
Advanced Capabilities

- **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.

3.2.21.1 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.

3.2.21.2 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=ASampleAYmx1ZXNxdWlycmVsLmNvbSx0cm9uYmxhMessageob28uY29tLDAzMDUwTjEyMTgxNjczMg==

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.

3.2.21.3 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
```

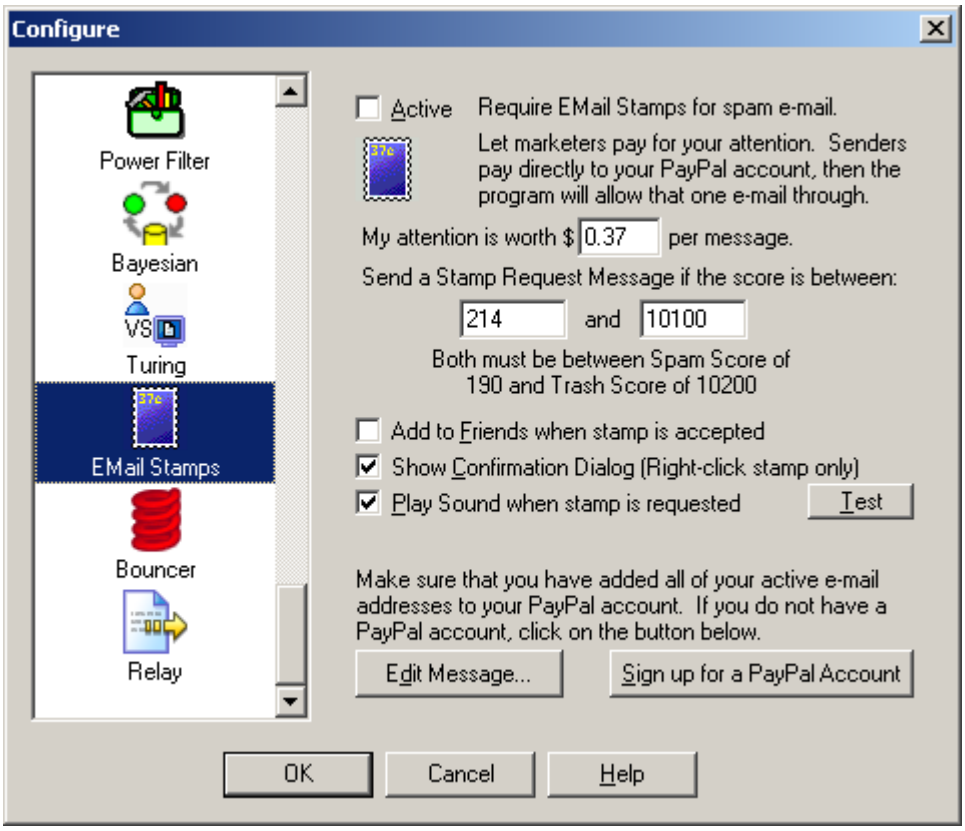
3.2.22 EMail Stamps

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.

3.2.22.1 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

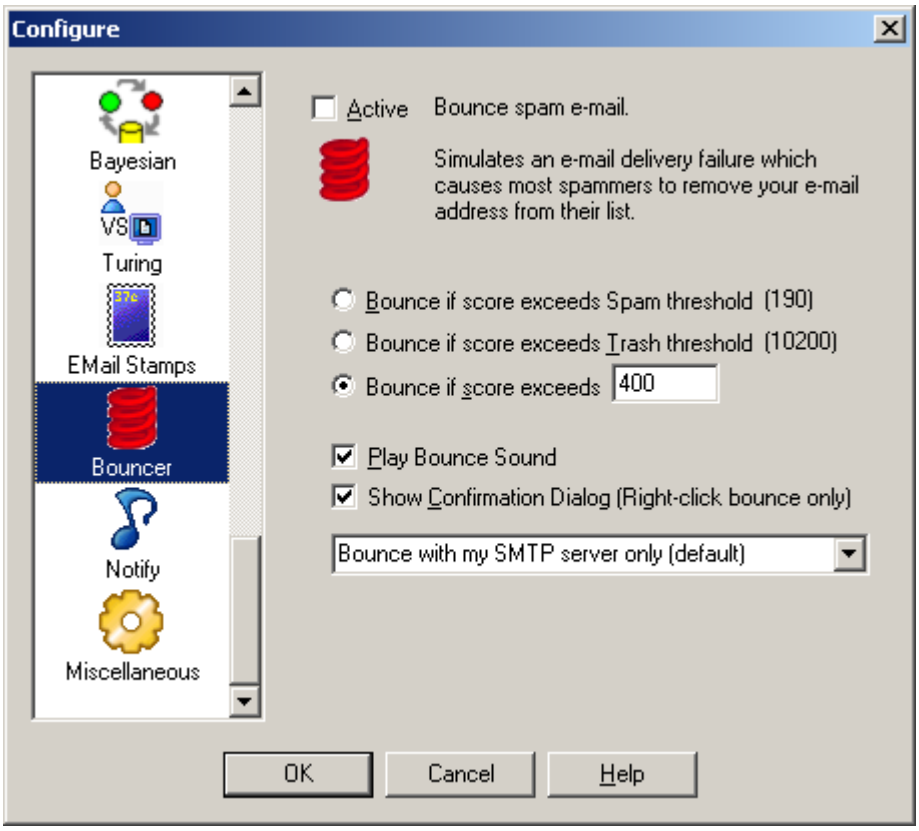
Sign up for PayPal

3.2.23 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.

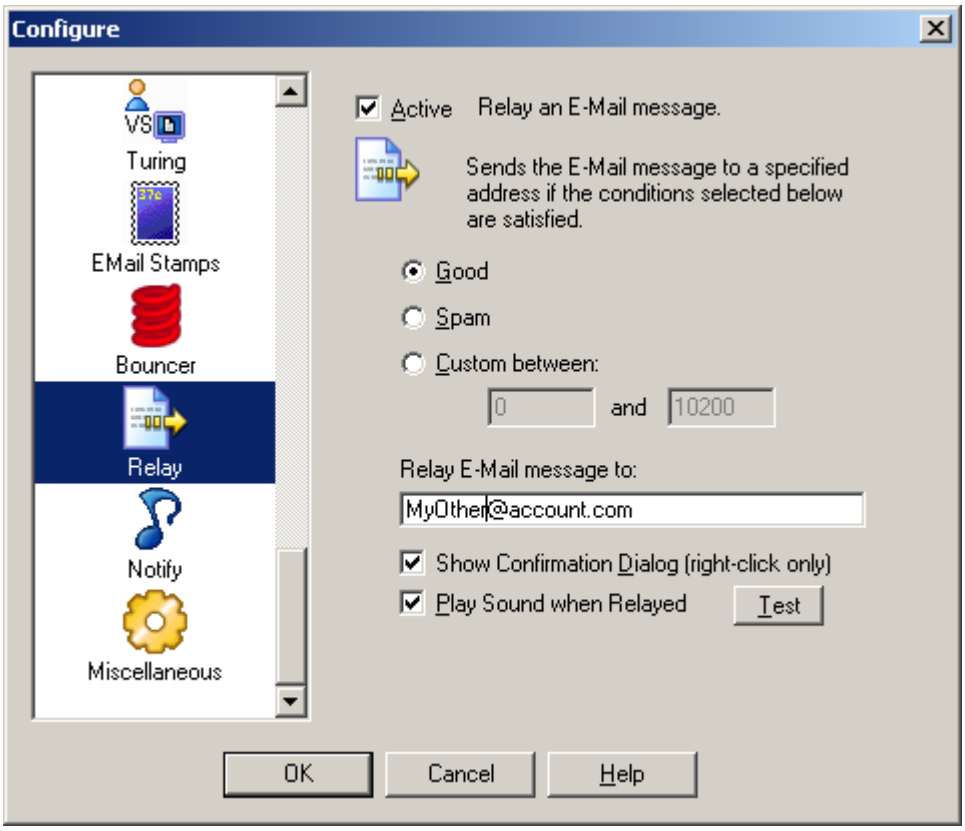
Bounce Method:

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** *EMail Stamps*, **or** *Bouncer*, but you should only turn on one of them.

3.2.24 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

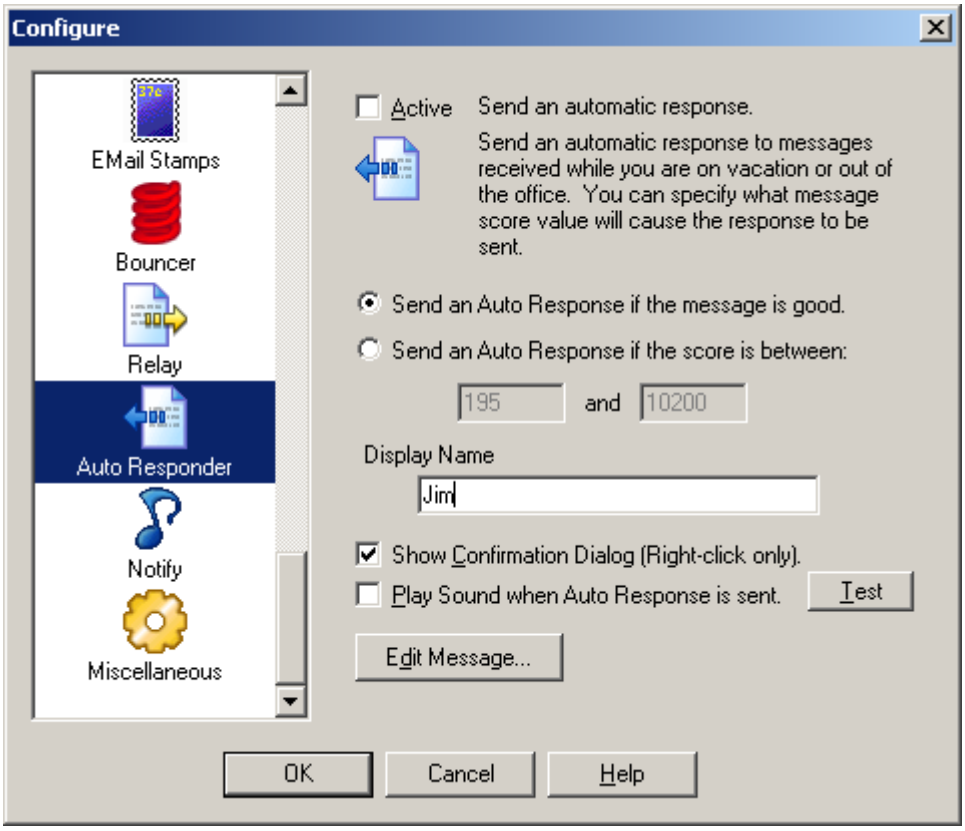
Relay E-mail message to: - Set the e-mail address of a valid e-mail account.

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.

3.2.25 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.

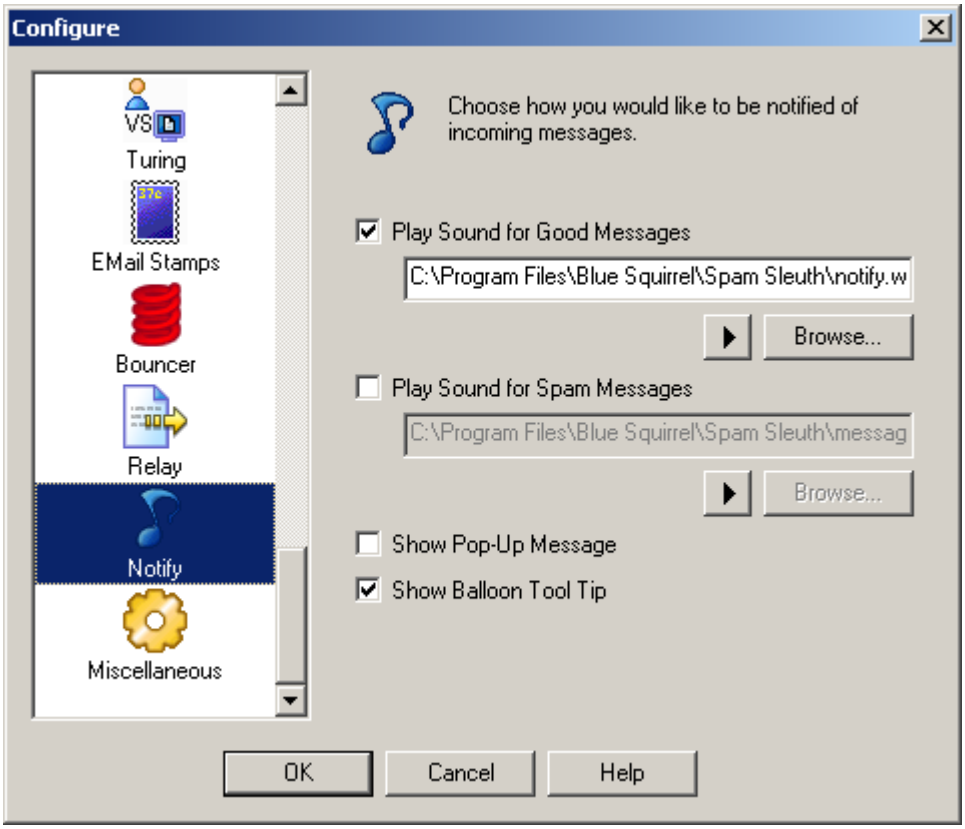


The Auto Responder sends an automatic message. A default message is included, but you can edit it to say whatever you'd like. The message will go back to the sender as listed in the From: or Reply To:.

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.

3.2.26 Notify



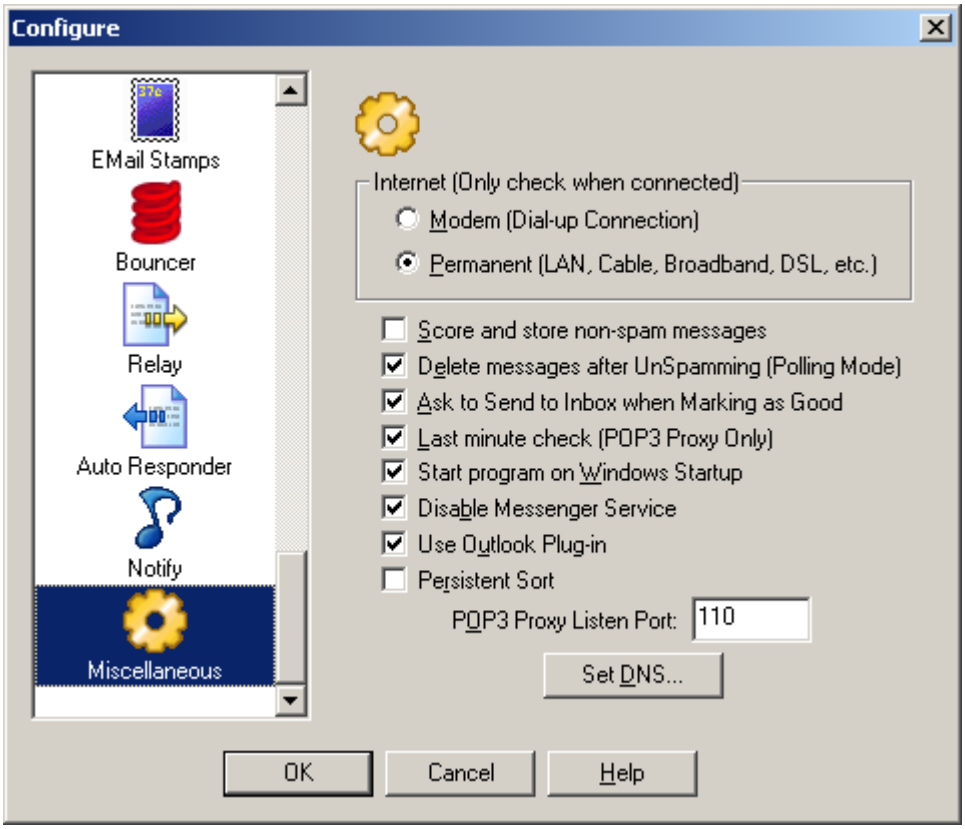
Choose how you would like to be notified of incoming messages.

You may select different sounds by choosing a different .WAV file for notification.

Show Pop-Up Message - shows status message when the Mail Jail is open and you check for e-mail.

Show Balloon Tool Top - Shows message when your mouse hovers over the icon in your system tray.

3.2.27 Miscellaneous



Setting the Internet Connection changes the behavior of Spam Sleuth . When you set **Modem (Dial-up Connection)**, Spam Sleuth will only check for spam while you are online. If you set Internet Connection to **Permanent**, it will check on the interval that you set, and it will attempt to initiate an Internet connection if you are not connected.

Score and store non-spam messages - Selecting this option will cause Spam Sleuth to keep all messages that it analyzes. It is a very helpful option for tuning and figuring out why an e-mail was not caught as spam. With this option selected, each e-mail will get a report whether it is spam or not. Messages not exceeding your spam threshold will have green dots next to them.

Delete Messages After UnSpamming (Polling Mode) - Will delete the message from Spam Sleuth once the message has been successfully re-mailed to your e-mail server. Keeps you from having two copies of a message. (For POP3 Proxy Mode, you would turn on/off 'Score and store non-spam messages')

Ask to Send to InBox when Marking as Good - You have the option to Mark messages as Good. You would do this for two reasons:
1. To have them delivered to your InBox
2. To correct the message before training the Bayesian Analyzer.

The program will default to asking you each time whether you want the message sent to your InBox. If you always want it sent to your InBox, then check this option.

Last minute check (POP3 Proxy Only) – If you are using POP3 Proxy mode where Spam Sleuth acts as your e-mail server, you can check this option to cause Spam Sleuth to go and check e-mail from your ISP's e-mail server right before it provides the e-mail to your e-mail program. This is the default. When this is on, you don't have to store your e-mail password with Spam Sleuth . Spam

Sleuth can take the password from your e-mail program and pass it along to your e-mail server.

Start Spam Sleuth on Windows Startup – Adds Spam Sleuth to the StartUp menu in Windows so that it will always be running. When you choose this option, you will be asked whether you want to check for e-mail immediately on StartUp. If you have a permanent connection and your personal firewall runs first, then you can answer YES to this question. Modem users should answer NO.

Disable Messenger Service - Windows 2000 and XP listen on port 139 for message notifications. It is ordinarily used for printer notifications and server shut-down notifications. Spammers have used this service to send messages. Checking this box will disable the service so you don't get these spam dialog messages.

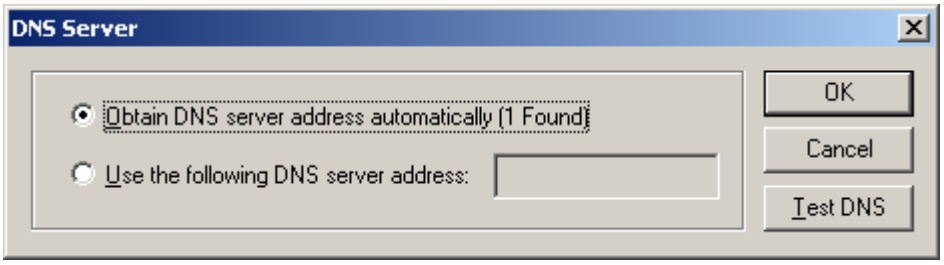
Use Outlook Plug-in - If you have Outlook (not Outlook Express), you can enable the Outlook Plug-in. The Outlook Plug-in lets you "Add to Friends" and "Add to Spammers" right from your Outlook toolbar. This option will not be available if Outlook is not detected on your system.

Persistent Sort - If you choose to sort your e-mail a different way, choosing will hold the setting so that the sort will happen each time you load the program. Loading up Spam Sleuth the first time may take a lot longer as the junk is highly compressed and it takes time to sort it. We don't recommend using this setting.

POP3 Proxy Listen Port – The port that Spam Sleuth listens to when in POP3 Proxy mode. The default for POP3 is 110. Unless another server is using port 110, you should not change this.

Set DNS - Sets the DNS Server that Spam Sleuth will use.

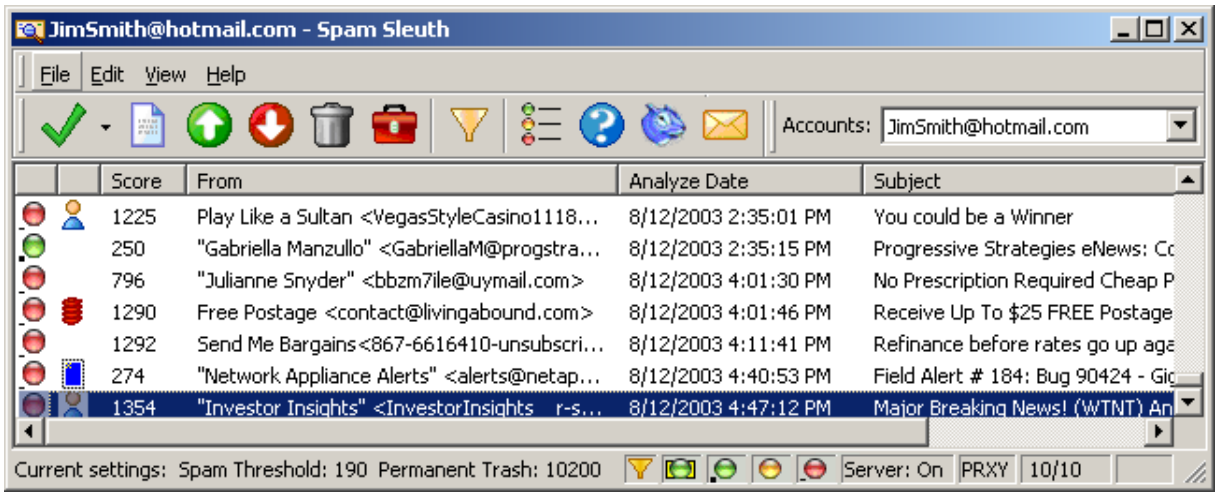
3.2.27.1 Set DNS...



DNS stands for Domain Name Server. It is the IP address of the computer that turns names like 'www.joeserver.com' into an IP address like '192.168.1.1'

Set the DNS that Valid Sender, Bouncer, and EMail Stamps will use to deliver e-mail. Usually the default automatic detection works fine. If not, you have the option to set your DNS server. You can use the Test DNS button to test the default automatic detection or your own custom DNS setting.

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.

 There is a green dot on a closed envelope to represent a non-spam message that is waiting on the server. If the message is in an account that is set to "POP3 Proxy" then the server is Spam Sleuth . If you are in a polling-mode, then the message is on your ISPs server. In polling-mode, if your e-mail program gets e-mail off of the server, this status will be updated the next time Spam Sleuth checks the server.

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.

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

 - Checks the active e-mail account for spam.

 - 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.

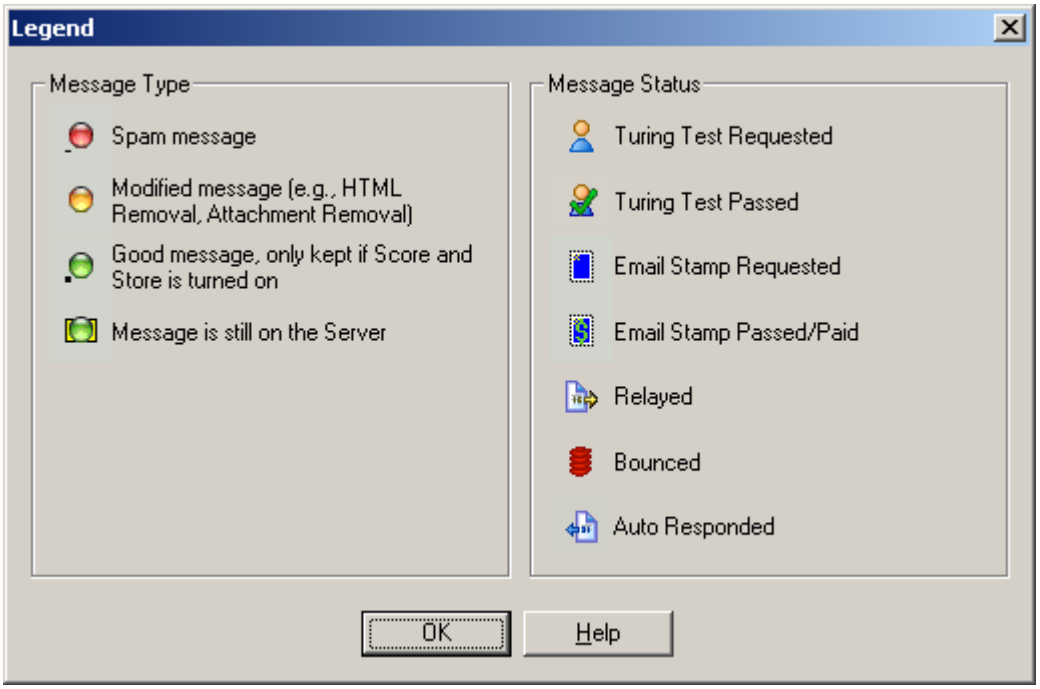
 - Launches the Configuration dialog box.

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.

Message is still on the Server - This indicates that the e-mail message is still on your e-mail server. If you are in POP3 Proxy Mode, then this means that Spam Sleuth is ready to deliver this message to your e-mail program. If you are in Polling Mode, this means that the last time Spam Sleuth checked with the server, the message was still there waiting for your e-mail program to download it.

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 Status Bar

The status bar at the bottom of the Mail Jail gives you information about the status of Spam Sleuth .

 This icon indicates that the filter is on.

It shows you your current Spam Threshold Score, and your Permanent Trash Score.


These icons show you which types of messages you are currently viewing.

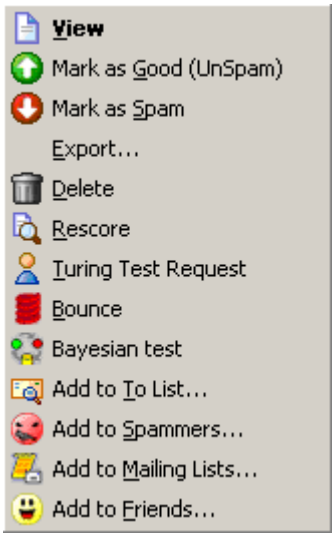
If any of your accounts are using POP3 Proxy, then Spam Sleuth shows you the server status. If none of your accounts are POP3 Proxy, then you will see "Server:Off" If you have POP3 Proxy accounts and the server is running, you will see "Server:On" If you have POP3 Proxy accounts and the server was not able to run because of a conflict with another program listening on port 110, then you will see "Server:Fail"

or
For the account that is selected in the upper right-hand corner, this lets you know whether the account is POP3 Proxy Mode or Polling Mode.

Shows you the number of messages visible, and the number of messages in the selected account(s). The number visible can be different because of your display options and the filter settings.

The last three are the standard CAPS, NUM, SCRL indicators found in many programs indicating the status of the CAPS Lock, Num Lock and Scroll Lock.

3.3.4 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. If you are in POP3 Proxy Mode, it will simply flag the e-mail to be re-delivered. If you are in Polling Mode, it will re-mail the message through the SMTP server you have configured.
Mark as Spam - You only need to use this if you intend to use the Bayesian Analyer. 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 Recyle 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. Rescore will not deliver the message to your inbox, or remove it from your server. Rescoring a message will give it a new score only.
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.

3.3.5 Menu

3.3.5.1 File

3.3.5.1.1 Configure...

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

3.3.5.1.2 Export...

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

3.3.5.1.3 Check Account

Checks one account or all accounts.

3.3.5.1.4 EMail Client

Launches your default e-mail program.

Will use the mailto: from your computer's configuration, or you can set the entry in your SpamSleuth.INI:

```
[General]
EMailClient=[path to your e-mail program]
```

3.3.5.1.5 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.

3.3.5.2 Edit

3.3.5.2.1 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.

3.3.5.2.2 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.

3.3.5.2.3 Mark as Good (UnSpam)

Delivers the message to your InBox.

Sends the e-mail back to your e-mail program. If you are in POP3 Proxy Mode, it will simply flag the e-mail to be re-delivered. If you are in Polling Mode, it will re-mail the message through the SMTP server you have configured.

3.3.5.2.4 Mark as Spam

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

In POP3 Proxy Mode, you can also use it before your e-mail client gets e-mail.

3.3.5.2.5 Select All

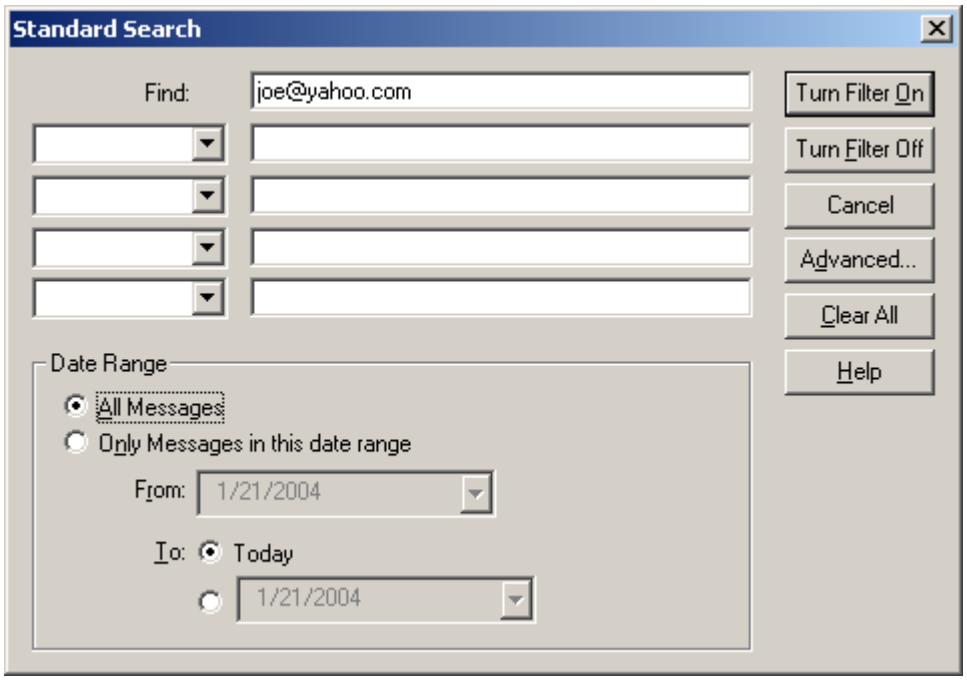
Selects all the messages in the Mail Jail.

3.3.5.2.6 Filter...

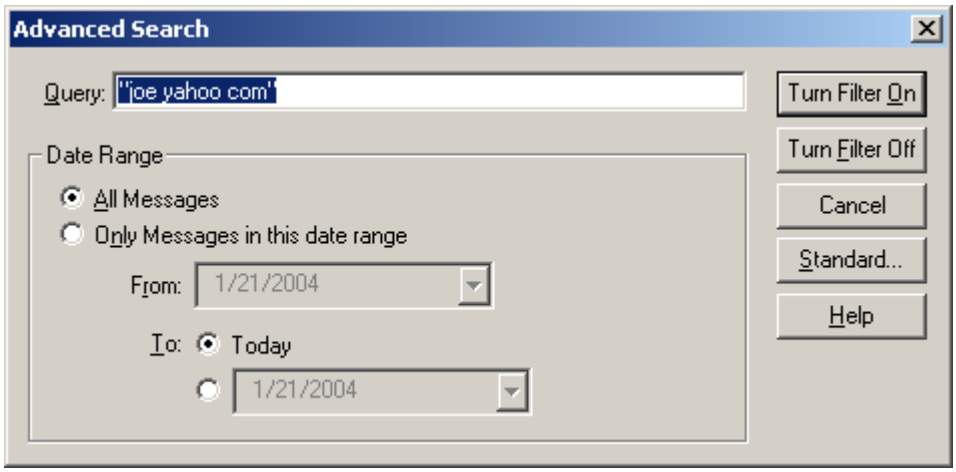
This menu option turns the filter on or off. The filter indexes your messages and lets you find a message that Spam Sleuth might have missed, or that you were expecting.

Each time you use the filter, the program will index the messages that have not yet been indexed. If the index it 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.



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.



3.3.5.2.7 Add to Friends...

Adds the e-mail address from the selected message to the Friends Analyzer.

3.3.5.2.8 Add to Mailing Lists...

Adds the e-mail address from the selected message to the Mailing Lists Analyzer.

3.3.5.2.9 Add to Spammers...

Adds the e-mail address from the selected message to the Spammers Analyzer.

3.3.5.2.10 Add to To List...

Adds the e-mail address from the selected message to the To Analyzer.

3.3.5.2.11 Bayesian Test

Does a test of the message using the statistical Bayesian Analyzer.

3.3.5.2.12 EMail Stamp Request

Requests an EMail Stamp using the EMail Stamps Analyzer.

3.3.5.2.13 Bounce

Manually bounces the message using the Bouncer Analyzer.

3.3.5.3 View

3.3.5.3.1 Toolbar

Turns on/off the toolbar.

3.3.5.3.2 Status Bar

Turns on/off the status bar at the bottom.

3.3.5.3.3 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.

3.3.5.3.4 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.

3.3.5.3.5 View Message

Views the selected message in a safe viewer.

3.3.5.3.6 Legend

Displays the legend for the icons.

3.3.5.4 Help

3.3.5.4.1 Help Topics

Opens the help for the program.

3.3.5.4.2 Update

- **Update Now!** - Checks with the Blue Squirrel update server for new updates to the program.
- **Undo Last Update...** - Will undo the changes made by the last update. Same as running IUNDO.EXE
- **Update Settings...** - Lets you frequency of checking for updates, and set Proxy settings if required for your network.

3.3.5.4.3 About...

Shows version number and information about the program.

4 Advanced Features

4.1 Instant Update

Spam Sleuth ™ includes our InstantX technology which gives you the ability to download updates over the Internet. First open the Mail Jail by double-clicking on the Spam Sleuth ™ icon  in your Windows System tray next to the clock. Choose Help > Update > Update Now!

Update Options

You can have Spam Sleuth ™ check for updates every time it runs, once a day, or once a week. From the menu select Help -> Update -> Settings -> InstantUpdate tab. Then you can specify how frequently to check for updates. We recommend once a day or once every seven days. If you don't want Spam Sleuth ™ to update at all, just set to Manual Update Only.

4.2 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.

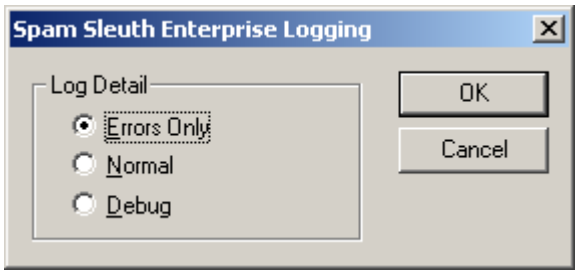
Spam Sleuth displays color coded dots next to the messages in the Mail Jail.

- 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.

4.3 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.

4.4 Hidden Settings

Occasionally there are settings that are needed, but are not often used. These settings require editing the SpamSleuth.INI file. The SpamSleuth.INI file is stored in the directory you chose to save the program during the installation wizard. By default the SpamSleuth.INI file is stored in C:\Program Files\Blue Squirrel\Spam Sleuth \SpamSleuth.ini.

```
[<e-mail>]   ;The section name is your e-mail name, configured for each account
SMTPPort=25  ;Override the default SMTP port of 25

[<e-mail>]   ;The section name is your e-mail name, configured for each account
UseSMTPAuthorization=1          ;0 will turn off SMTP authorization on ESMTP
servers

KeepOriginalSender=0  ;  Setting this to 0 causes the program to use your e-mail
address as the MAIL FROM: address when UnSpamming messages or sending a modified
message.  Setting this option 1 cause Spam Sleuth  to use the original sender's e-
mail address in the MAIL FROM:

EMailClient=   ;Set this to the full path of your e-mail program if the launch e-
mail button doesn't work.


[General]
AskToClose=0  ;0=ask, 1=continue, 2=close

[General]
Pop3ProxyDeleteFromServer=1    ;0 keeps Spam Sleuth  from removing e-mail from the
server.  If you change this, your e-mail box may fill up at your ISP.  Only applies
to good messages (spam messages are always deleted).  Useful for viewing e-mail at
home and on a web account.

[General]
DeleteFromServer=1    ;Starting with version 3.0, the Polling Mode will delete
messages from the server if you mark them as spam or delete them.  Setting this
setting to 0 will keep Spam Sleuth  from doing this.

[General]
RunAfter=<Full path to a program>   ;This option combined with the /CheckAll and
/RunAfter command-line options will cause Spam Sleuth  to run a program such as an
e-mail reader after it has scanned the active e-mail accounts.

[General]
Pop3ProxyLocalOnly=1     ;0 allows any computer to use your POP3 Proxy server   DO
```

NOT CHANGE THIS UNLESS YOU UNDERSTAND THE SECURITY RISKS!

4.5 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.

For example, `"C:\Program Files\Blue Squirrel\Spam Sleuth \SpamSleuth.exe" /NoSplash`

- **`/NoSplash`** – This option keeps the Splash Screen from appearing on start up.
- **`/CheckAll`** – Starts checking e-mail immediately upon startup. If this option is not set, it will wait for the specified amount of time before checking e-mail.
- **`/Delay:3`** - Pauses all Internet activity (Update checking and e-mail scanning) for 3 minutes (set any number you want). The program will not appear until the time has expired. Use this if your computer doesn't make an Internet connection right away.
- **`/X`** – Exits the program after it checks for Spam – only works when `/CheckAll` is specified
- **`/RunAfter`** – If this is passed it will check for `RunAfter=`<program> in the [General] section of SpamSleuth`.INI` and will run the specified program.
- **`/NoMinimize`** – This keeps Spam Sleuth from minimizing to the tray when you run it. It also keeps Spam Sleuth from temporarily hiding off-screen while it loads the spam messages.

4.6 Web E-Mail

Spam Sleuth only works with POP3 e-mail servers. You can use additional software that will translate web e-mail for Spam Sleuth , giving you the option to use Spam Sleuth with free Yahoo and HotMail accounts. Use Web2POP to use Spam Sleuth with Yahoo, Excite, AOL, or Hotmail. Configure the POP3 Server setting in Spam Sleuth to localhost. For more information see the Getting Started portion of this manual.

4.7 Proprietary E-Mail

Spam Sleuth works with POP3 e-mail servers. Some e-mail systems are proprietary. The two biggest proprietary systems are MSN and AOL. You can use Web2Pop (http://www.bluesquirrel.com/products/web2pop) to work with Hotmail, MSN, Yahoo, AOL and many other web e-mail accounts.

4.8 Tips and Tricks

4.8.1 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 Mail Jail window must be open.

- **ESC** – Minimizes the Mail Jail window.
- • **F5** – Checks e-mail in active account.
- **F4** – Changes the active account in the Mail Jail.
- **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.
- **CTRL-ALT-W** – Launches the first-time Wizard for automatically configuring e-mail accounts.

4.8.2 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.

4.8.3 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 Troubleshooting

Most of the time Spam Sleuth will install and begin working immediately. In some rare cases, it may be necessary to troubleshoot. This interactive troubleshooter will take you through a step-by-step process to determine why Spam Sleuth isn't working. Just follow the links.

Choose your problem:

I'm getting e-mail, but the program isn't screening out spam.
I'm not getting e-mail anymore, I think the anti-spam program is blocking it.
Too much spam is being let through.
My good messages are blocked.
The program is working, but is less effective than before.
The anti-spam program can check e-mail, but my e-mail program doesn't get e-mail.I use AOL, Hotmail, free Yahoo, Excite, or another free web mail program.
I use MSN and I can't get your program to work.
I use free Juno, and I can't get your program to work.
I'm having trouble with Web2POP

5.1 Troubleshooting-PollingVsProxy

Spam Sleuth works two different ways. It can run Polling or POP3 Proxy. Click here to see the differences.

Choose One:

Polling Mode
POP3 Proxy Mode

How to tell:
1. Go to File->Configure.../Accounts
2. Choose your account and hit [Edit]
3. At the top of the Edit Account dialog one of the modes will be selected.

5.1.1 POP3ProxyMode

You are running Spam Sleuth in POP3 Proxy Mode. You need to check to make sure a few things are set.

Check to make sure:
1. At the bottom of Spam Sleuth in the status area, it should say "Server:On"
2. At the bottom of Spam Sleuth in the status area, it should say "PRXY". If it does not say "PRXY" and you have more than one account configured, then choose your account from the drop-down in the upper right-hand corner, and make sure it says "PRXY".

Choose one:

It says "Server:On" and "PRXY" like it is supposed to.
It says "Server:Off"
It says "Server:Fail"
It says "POLL"

5.1.1.1 Server OK

It sounds like the POP3 Proxy server is running just fine. If you want to do an additional test on the POP3 Proxy, click here. Let's check to make sure that Spam Sleuth can get your e-mail.

Steps:
1. Go to File->Configure.../Accounts and choose your account.
2. Hit the "Test POP3" button and make sure Spam Sleuth connects to your e-mail server.
3. Hit the "Test SMTP" button and make sure Spam Sleuth connects to your e-mail server.

Choose One:
It is working now.
The "Test POP3" works, but I still don't get my e-mail in my e-mail program.
The "Test POP3" fails.
The "Test SMTP" fails.

5.1.1.1.1 Test POP3 Fails

If the "Test POP3" fails it can be for several reasons:

1. **You are not connected to the Internet.** If you don't see any text show up in the test box, make sure you have a good connection to the Internet. Make sure you can browse to web sites without errors.
2. **Your "Incoming (POP3) Server" is wrong.** Check to make sure that you have the right information in the "Incoming (POP3) Server" field. This is usually supplied with your ISP account. It would also be the information that was in your e-mail program. If Spam Sleuth changed the information, it would be logged in the AutoConfigure.log in the Spam Sleuth program directory. If you are using Web2POP, this should be 127.0.0.1.
3. **Your username is not valid.** The "Test POP3" shows you the conversation between Spam Sleuth and your e-mail server. If it gets an error when sending the USER, then check your username, and make sure it is correct. Some e-mail servers require your full e-mail address for Username, but most just require the part before the '@' symbol.
4. **Your password is not valid.** It gets an error after it sends PASS, check to make sure your password is valid, and that you've filled in a password for the account. You will never see the password sent because we don't show it in the conversation. This is normal.
5. **Your POP3 Server requires APOP.** If you are certain that your username and password are set correctly, but it is still not connecting properly, your server may require APOP. Hit OK, then hit [Advanced] and select "Use APOP Authentication"

Choose One:

It works now.
I have checked all of the above and "Test POP3" still fails.

5.1.1.1.2 Test SMTP Fails

If the "Test SMTP" fails it can be for several reasons:

1. **You are not connected to the Internet.** If you don't see any text show up in the test box, make sure you have a good connection to the Internet. Make sure you can browse to web sites without errors.
2. **Your "Outgoing (SMTP) Server" is wrong.** Check to make sure that you are using the settings you were given by your ISP, or those that were in your e-mail program. It would be the same setting as your e-mail program.
3. **Your SMTP Server requires authentication.** If you get a message in the "Test SMTP" that your server requires authentication, then hit OK, then hit the [Advanced] button and turn on "SMTP

Authentication" If it uses the same user/pass as your POP3 server, then you can leave the other settings blank, otherwise fill them in with user/pass for SMTP.

Choose One:

It works now.
I have checked all of the above, but "Test SMTP" still fails.

5.1.1.1.3 Troubleshooting-ClientTest

The problem probably lies with the settings in your e-mail program.

Now we need to check your e-mail settings:

Steps:
1. Go to your e-mail program's account settings
2. Check to make sure that the Incoming (POP3) Server is set to 'localhost' or 127.0.0.1 Note: If it was set to **localhost**, try setting it to 127.0.0.1 (both should work, but we've found that 127.0.0.1 often works when **localhost** doesn't.
3. If you have more than one account with the same username (Example: joe@verizon.com, joe@bellsouth.com), then make sure your full e-mail address in in the "Username" in your e-mail program.

Choose One:

It is working great now.
I've set my setting in my e-mail program and it still doesn't work.

5.1.1.1.4 Additional POP3 Proxy Test

Here is an additional test you can do to check the POP3 Proxy:
1. Go to Start->Run
2. Type in "COMMAND[ENTER]" if you are using Windows 95/98/ME, or type in "CMD[ENTER]" if you are on NT/2000/XP
3. You should get a command prompt.
4. Type "TELNET 127.0.0.1 110[ENTER]"
5. A response should come back like "Blue Squirrel Proxy Ready"
6. Type "QUIT[ENTER]" to disconnect from the POP3 Proxy
7. Type "EXIT[ENTER]" to close the command prompt.

Choose One:

It works now.
I get "Blue Squirrel Proxy Ready" but my e-mail still doesn't work.
I get nothing after the entering the TELNET line.
I get something else after entering the TELNET line.

5.1.1.2 Server Off

This is a very unusual case. Please check that you have POP3 Proxy turned on.

5.1.1.3 Server Fail

This is a problem that must be solved to use POP3 Proxy Mode.

There are a few reasons you might get "Server:Fail"

Choose One:

I have a personal firewall, like Zone Alarm, Norton Security Suite, etc.
I have an anti-virus program that works the same way that does, and it is using Port 110.
I have another anti-spam program that works the same way that and it is using Port 110.

5.1.1.3.1 Troubleshooting-Firewall Conflict

Personal Firewalls are designed to protect your computer against unauthorized access. However, in POP3 Proxy Mode, it is normal for Spam Sleuth to install as a server and listen on port 110. Most personal firewall programs will notify you when this is happening the first time and give you the option to allow it, or reject it. If you've rejected Spam Sleuth , then you'll need to find the settings in your personal firewall and allow Spam Sleuth to run as a server. Spam Sleuth will only allow connections from your own machine so it is safe to allow Spam Sleuth to listen on port 110.

Choose One:

I've allowed it to run as a server, but I still get "Server:Fail"
I've disabled my personal firewall, but I still get "Server:Fail"
It is working great now.

5.1.1.3.2 Troubleshooting-Anti Virus Conflict

Some anti-virus programs work the same way that Spam Sleuth does. They run a server at port 110. Since only one application can be a server listening to port 110, and you probably want to keep your anti-virus software, we need to listen on a different port. Spam Sleuth can do this. There are two ways change the configuration -- automatic or manual. Automatic works most of the time, but here are both methods.

Automatic reconfiguration steps (recommended):

1. Close your e-mail program.
2. In Spam Sleuth , go to File->Configure.../Accounts and remove the account. You should get a message about the account information being removed from your e-mail program.
3. In Spam Sleuth , go to File->Configure.../Miscellaneous and set the Listen Port to 109.
4. Hit CTRL-ALT-W to run the automatic configuration wizard, and choose your e-mail account, and Spam Sleuth will reconfigure your e-mail program to use port 109. If your e-mail account isn't listed, then go to the manual configuration steps.

Manual configuration steps (if necessary, after following automatic steps above):

1. Open your e-mail program and check to make sure all the setting are back to the original settings. If your e-mail program is using the anti-virus program on port 110, then this means your e-mail program will have settings that cause your e-mail program to get e-mail from your anti-virus program.
2. Make sure your e-mail is working properly (without Spam Sleuth)
3. Write down the settings from your e-mail program for "Username", "Incoming (POP3) Server", and "Outgoing (SMTP) Server"
4. In Spam Sleuth , go to File->Configure.../Accounts and ADD the account and enter the information from your e-mail program.
   - Mode: "POP3 Proxy Mode"

- EMail Address: Enter your e-mail address
- Incoming (POP3) Server: Enter the information from your e-mail program that you wrote down.
- Username: Enter the information from your e-mail program that you wrote down.
- Password: You can fill it in, or leave it blank. It will get it from your e-mail program.
- Outgoing Server (SMTP): Enter the information from your e-mail program that you wrote down.
- Check Every: Leave it at 0

5. Go back to your e-mail program and set "Incoming (POP3) Server" to 127.0.0.1, and username to your full e-mail address as you entered in the step above.

Choose One:

Still not working.
It is working great now.

5.1.1.3.3 Troubleshooting-Anti Spam Conflict

We don't recommend running two anti-spam solutions. Please uninstall the other anti-spam solution and use Spam Sleuth exclusively.

Choose One:

Still not working.
It is working great now.

5.1.1.4 POLL should be PRXY

If it says POLL in the status area, when it should say PRXY, go to File->Configure.../Accounts and make sure the accounts you want to be POP3 Proxy Mode are set that way. Then make sure that you choose the correct account from the drop-down in the upper right-hand corner of the Mail Jail.

Choose One:

It is working now.
It still says POLL, when it should say PRXY.

5.1.2 Polling Mode - Not getting e-mail

You are running in Polling Mode. In this mode, Spam Sleuth does not affect the normal flow of e-mail. Your e-mail program will get e-mail just as it has before. For Spam Sleuth to be effective, it must check for e-mail before your e-mail program, and remove the bad (spam) e-mail from your e-mail server before your e-mail program checks for e-mail. We recommend POP3 Proxy Mode for most people. Click here for more information on the pros and cons of use Polling Mode.

In Polling Mode, Spam Sleuth does not affect whether your e-mail program can get e-mail. If you have switched between POP3 Proxy Mode and Polling Mode, it is possible that the settings in your e-mail program have been changed. Please change them back to the original settings. When you use Polling Mode, no changes are necessary to your e-mail program. If you suspect that Spam Sleuth has changed your setting and you don't know what they are, there is an AutoConfigure.log file in the Spam Sleuth program directory which logs all the changes made to your e-mail program.

Check One:

I've set my e-mail settings back to their original settings and everything is working.
I can get e-mail now, but I have other problems.

5.1.3 Polling Mode - Not Screening Spam

If you are in Polling Mode, and Spam Sleuth is not screening spam, then you need to check these things:

1. Make sure the setting in Spam Sleuth under File->Configure.../Accounts is the same as the information in your e-mail program.
2. Make sure that Spam Sleuth is set to check for spam periodically. Go to File->Configure.../Accounts, choose your account and hit [Edit] and make sure that "Check Every" is set to 5 minutes or so.
3. Make sure that Spam Sleuth checks for e-mail before your e-mail program does. If you need to, open Spam Sleuth and select the green check box in the toolbar before checking e-mail with your e-mail program.

Choose One:

It is working now.
It still doesn't screen spam.

5.2 Not Screening Spam

Spam Sleuth may not be screening out spam because the settings are out-of-whack, or because it is not "seeing" the e-mail.

To check whether or not Spam Sleuth is "seeing" the e-mail:

1. Go to File->Configure.../Miscellaneous and turn on "Score and store non-spam messages" so that all messages seen will be stored.
2. Go to File->Configure.../Score and make sure the Permanent trash level is 22000 or higher.
3. Go to View->Display and make sure all message types are selected.
4. When Spam Sleuth checks for mail, you should see messages appear in the Mail Jail.

If messages are appearing in the Mail Jail, double-click on the messages to see what type of scores they are getting. If the scores are negative, it probably means that your e-mail address is in MailingLists, or a wildcard entry is in Friends. The spam report should tell you what is giving the negative score. If the scores are normal (ranging from -20,000 for Friends e-mail, to +12,000 for spam messages), then check File->Configure.../Score to make sure the spam score is 190 (the default).

If messages are NOT appearing in the Mail Jail, it could be for several reasons:

1. Spam Sleuth is configured as POP3 Proxy, but your e-mail program is going straight to the server, and not triggering Spam Sleuth . You should Troubleshoot POP3 Proxy Mode.
2. Spam Sleuth is configured as Polling, but the "Check Every:" is set to 0, so it never checks. Go to File->Configure.../Accounts and choose the account and hit [Edit] and set "Check Every" to 5 minutes.
3. Spam Sleuth is configured for Polling but is configured wrong, so it never gets a chance to clean out your e-mail. Go to File->Configure.../Accounts and go to each account and use the "Test POP3" button. Make sure the information is the same as your e-mail program.

Choose One:

It is working now.
I have done all the steps above and it still is not working.

5.3 Too much spam

Spam Sleuth is pretty good at detecting spam with the default settings. It should be detecting 80% to 95% of the spam. While it is possible to configure Spam Sleuth to get 100% of the spam, it is usually not worth your time to continually tune Spam Sleuth to achieve 100% effectiveness.

Start by going to File->Configure.../Miscellaneous and turning on 'Score and store non-spam messages'. This will let you see a report for all messages that Spam Sleuth sees, including the ones that aren't tagged as spam. You can double-click on any message to get a report for what was found in the message.

Things to check:
1. Look at the report for the messages and see what is giving or deducting points. If the points assigned are negative, find out why. Only Friends, MailingLists, GoodWords, and Bayesian should deduct points.
2. Make sure you haven't added your own e-mail address to MailingLists. Go to File->Configure.../MailingLists and make sure your own e-mail address is not listed.
3. Make sure you haven't added a wildcard entry in Friends like *@.COM which would allow all senders with an e-mail ending in .COM.
4. You may want to increase the points given by some of the analyzers. Go to File->Configure... and then choose the analyzer and then increase the points for the item that needs more points.

Choose One:

It works now.
It seems that some of the e-mail isn't beeing screened.
None of the e-mail is being screened.

5.4 Good Messages Blocked

It is always possible that good messages will be blocked. These are called "false positives" Here are some ways you can decrease your false positives:

1. Add the e-mail addresses of your friends to your Friends list. Go to File->Configure.../Friends and add their e-mail addresses. You can import them from some e-mail programs.
2. Add the return e-mail address of mailing lists to your Friends list.
3. If the return address is always different for a particular mailing list, then you can add the "To:" address of the mailing list to Mailing Lists. Go to File->Configure.../MailingLists to add it.
4. If you work in a certain industry, there are probably words that occur often in your e-mails, that don't ordinarily occur in spam. Perhaps certain medical terms if you are a doctor, or engine part terms if you are mechanic. Add these words to your GoodWords list. Go to File->Configure.../GoodWords. Type in a word, and give it points. These points will be deducted from to point total of the e-mail.

Choose One:

It works now.
All of my good e-mail is being blocked.
All of my e-mail (good and spam) is being blocked.

5.5 Less Effective

It is possible for some settings to get out-of-whack. Depending on whether Spam Sleuth is letting in too much spam, or blocking too much good e-mail, there are different ways to fix the settings.

Choose One:

It is working now.
It seems to let in more spam.
It seems to block more good e-mail.

5.6 Non-POP3 E-Mail Server

If you have an e-mail account that does not support POP3, then you may need some additional gateway software so that Spam Sleuth can screen your e-mail.

I Use:

AOL
MSN
Yahoo
Hotmail
Excite
Other Web EMail
Free Juno (no paid subscription)

5.6.1 AOL

You can use AOL with Spam Sleuth , provided you also have Web2POP (http://www.bluesquirrel.com/products/web2pop/)

To configure:

1. Install Web2POP, and make sure it is always running in the system tray.
2. In Spam Sleuth , go to File->Configure.../Accounts, and Add account
3. Set to "Polling Mode".
4. Set the e-mail to your e-mail address.
5. Set the "Incoming (POP3) Server" to 127.0.0.1
6. Set the Username to your full e-mail address.
7. Set the Password to your e-mail password
8. Set the Outgoing (SMTP) Server to mailin-01.mx.aol.com
9. Set the "Check Every" to 5 minutes

Changes if you want to use your favorite e-mail program instead of the AOL client:

1. Right-click on Web2POP and choose Options, and set "Listen to Port" to 109
2. In Spam Sleuth , go to File->Configure.../Accounts, choose your account, hit [Edit]:
   - Set to "POP3 Proxy Mode"
   - Set "Check Every" to 0
   - Hit [Advanced] and set the Port to 109.

5.6.2 MSN

You can use MSN with Spam Sleuth , provided you also have Web2POP (http://www.bluesquirrel.com/products/web2pop/)

To configure:
1. Install Web2POP, and make sure it is always running in the system tray.
2. In Spam Sleuth , go to File->Configure.../Accounts, and Add account
3. Set to "Polling Mode".
4. Set the e-mail to your e-mail address.
5. Set the "Incoming (POP3) Server" to 127.0.0.1
6. Set the Username to your full e-mail address.
7. Set the Password to your e-mail password
8. Set the Outgoing (SMTP) Server to mx1.hotmail.com
9. Set the "Check Every" to 5 minutes

Changes if you want to use your favorite e-mail program instead of the MSN client:
1. Right-click on Web2POP and choose Options, and set "Listen to Port" to 109
2. In Spam Sleuth , go to File->Configure.../Accounts, choose your account, hit [Edit]:
   - Set to "POP3 Proxy Mode"
   - Set "Check Every" to 0
   - Hit [Advanced] and set the Port to 109.

If you hit the "Test POP3" button in the Account configuration, and get the error "No support library found or library not capable", you need to add these lines to the Web2POP.INI file in the Web2POP program directory:

[domains]
msn.com=hotmail

5.6.3 Hotmail

You can use Hotmail with Spam Sleuth , provided you also have Web2POP (http://www.bluesquirrel.com/products/web2pop/)

To configure:
1. Install Web2POP, and make sure it is always running in the system tray.
2. In Spam Sleuth , go to File->Configure.../Accounts, and Add account
3. Set to "Polling Mode".
4. Set the e-mail to your e-mail address.
5. Set the "Incoming (POP3) Server" to 127.0.0.1
6. Set the Username to your full e-mail address.
7. Set the Password to your e-mail password
8. Set the Outgoing (SMTP) Server to mx1.hotmail.com
9. Set the "Check Every" to 5 minutes

Changes if you want to use your favorite e-mail program instead of the web:
1. Right-click on Web2POP and choose Options, and set "Listen to Port" to 109
2. In Spam Sleuth , go to File->Configure.../Accounts, choose your account, hit [Edit]:
   - Set to "POP3 Proxy Mode"
   - Set "Check Every" to 0
   - Hit [Advanced] and set the Port to 109.

5.6.4 Yahoo (free)

If you have the Yahoo subscription for a POP3 account, then these instructions do not apply. These instructions are only for the Free Yahoo which does not require a subscription.

You can use the free Yahoo with Spam Sleuth , provided you also have Web2POP (http://www.bluesquirrel.com/products/web2pop/)

To configure:
1. Install Web2POP, and make sure it is always running in the system tray.
2. In Spam Sleuth , go to File->Configure.../Accounts, and Add account
3. Set to "Polling Mode".
4. Set the e-mail to your e-mail address.
5. Set the "Incoming (POP3) Server" to 127.0.0.1
6. Set the Username to your full e-mail address.
7. Set the Password to your e-mail password
8. Set the Outgoing (SMTP) Server to mx1.mail.yahoo.com
9. Set the "Check Every" to 5 minutes

Changes if you want to use your favorite e-mail program instead of your web browser:
1. Right-click on Web2POP and choose Options, and set "Listen to Port" to 109
2. In Spam Sleuth , go to File->Configure.../Accounts, choose your account, hit [Edit]:
   - Set to "POP3 Proxy Mode"
   - Set "Check Every" to 0
   - Hit [Advanced] and set the Port to 109.

5.6.5 Excite

You can use Excite webmail with Spam Sleuth , provided you also have Web2POP (http://www.bluesquirrel.com/products/web2pop/)

You will also need to download the correct module for Web2POP from JMASoftware (http://www.jmasoftware.com/english/products/web2pop/search.asp)

To configure:
1. Install Web2POP, and make sure it is always running in the system tray.
2. In Spam Sleuth , go to File->Configure.../Accounts, and Add account
3. Set to "Polling Mode".
4. Set the e-mail to your e-mail address.
5. Set the "Incoming (POP3) Server" to 127.0.0.1
6. Set the Username to your full e-mail address.
7. Set the Password to your e-mail password
8. Set the Outgoing (SMTP) Server to xmxpita.excite.com
9. Set the "Check Every" to 5 minutes

Changes if you want to use your favorite e-mail program instead of your web browser:
1. Right-click on Web2POP and choose Options, and set "Listen to Port" to 109
2. In Spam Sleuth , go to File->Configure.../Accounts, choose your account, hit [Edit]:
   - Set to "POP3 Proxy Mode"
   - Set "Check Every" to 0
   - Hit [Advanced] and set the Port to 109.

5.6.6 Other Web Accounts

Spam Sleuth supports most web mail accounts provided you also have Web2POP (http://www.bluesquirrel.com/products/web2pop/)

You will also need to download the correct module for Web2POP from JMASoftware (http://www.jmasoftware.com/english/products/web2pop/search.asp)

To configure:
1. Install Web2POP, and make sure it is always running in the system tray.
2. In Spam Sleuth , go to File->Configure.../Accounts, and Add account
3. Set to "Polling Mode".
4. Set the e-mail to your e-mail address.
5. Set the "Incoming (POP3) Server" to 127.0.0.1
6. Set the Username to your full e-mail address.
7. Set the Password to your e-mail password
8. Set the Outgoing (SMTP) Server to an SMTP server that will let you send e-mail to yourself.
9. Set the "Check Every" to 5 minutes

Changes if you want to use your favorite e-mail program instead of your web browser:
1. Right-click on Web2POP and choose Options, and set "Listen to Port" to 109
2. In Spam Sleuth , go to File->Configure.../Accounts, choose your account, hit [Edit]:
   - Set to "POP3 Proxy Mode"
   - Set "Check Every" to 0
   - Hit [Advanced] and set the Port to 109.

5.6.7 Juno

If you have the Juno with a subscription fee, then you can configure Spam Sleuth as you would any POP3 account. Request the settings from Juno.

If you are using the Free Juno, then Spam Sleuth will not work, as the system is a proprietary system. Purchase the subscription Juno, or change to a different ISP.

5.6.8 SMTP Server for WebMail

If you have a web mail account, then you probably don't have an ISP that is supplying you with an SMTP server you can use. So what do you put in for the "Outgoing (SMTP) Server" in Spam Sleuth ?

In most cases (except for Bouncer, Turing and E-Mail Stamps), you only need to send e-mail to yourself to be able UnSpam messages.

If you have an SMTP server that you can use, go ahead and enter it. If not, you'll have to use one from the web mail that won't let you send mail except to yourself. In this case you won't be able to use Bouncer, Turing, EMail Stamps, or other analyzers that send out e-mail.

To find one:
1. In Windows, choose Start->Run...
2. If you have Windows 95/98/ME, type `COMMAND`[ENTER], if you use Windows NT/2000/XP, type `CMD`[ENTER] to get a command prompt.
3. At the command prompt, type `NSLOOKUP`[ENTER]
4. If that works, and you don't get an error, then type `SET TYPE=MX`[ENTER]
5. Then type your webmail domain, like this: `EXCITE.COM`[ENTER]
7. You should get a list of names that might look like this: `mx.excite.com`

Enter that name into the "Outgoing (SMTP) Server" field and hit the [Test SMTP] button. If it works,

then you can use it for your SMTP server.

5.7 Troubleshoot Web2POP

Web2POP is a third-party application which allows Spam Sleuth to work with non-POP3 servers.

You can purchase Web2POP with Spam Sleuth by visiting:
http://www.bluesquirrel.com/products/Web2POP/

Choose One:

Web2POP shuts down as soon as I run it.
Web2POP is not listening on the right port.
Web2POP says the module is not there.

5.7.1 Web2POP Shut Down

Spam Sleuth in POP3 Proxy Mode also uses port 110 (by default). We recommend that you move Web2POP to 109.

If Web2POP is running, then you can right-click on the Web2POP icon in the tray and choose Options, and then set the "Listen to Port" to 109.

If Web2POP shuts down when you run it, it is because the port it is trying to use (110 by default) is in use by another program. Web2POP will give you a message that says something is using the port and it is unable to initialize.

If Web2POP will not run, then you need to edit (or make) a `Web2POP.ini` file in the Web2POP program directory. It should have these lines:

```
[setup]
Port=109
```

5.7.2 Web2POP Module

Web2POP uses modules which connect to various types of e-mail servers. You need to make sure you are using the right module for your e-mail server.

If you use the "Test POP3" button and get "No support library found or library not capable" error, then Web2POP was unable to find a module for your e-mail address.

To find and download new modules:
(http://www.jmasoftware.com/english/products/web2pop/search.asp)

5.8 Troubleshooting-Working

Great! Thanks for choosing Spam Sleuth .

You may want to read more about how to eliminate spam.

5.9 Unable to Fix

Make sure that you have gone through the steps in the Troubleshooter.

If you are still unable to solve the problem, please follow these steps:
1. Turn on Debug logging with CTRL-ALT-L and set to Debug level.
2. Try to duplicate the problem again with Debug logging turned on. This step is important because we need to get a log of the problem occuring.
3. Open a trouble ticket by going to http://www.bluesquirrel.com/support, checking the FAQ for newer information, and if the answer is not there, let us know the specifics. We may request the log file if we cannot solve the problem right away.

6 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.

6.1 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.

6.2 Visit Our Web Site

Program Web Site:

http://www.bluesquirrel.com/products/SpamSleuth/

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/

6.3 Technical Support

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

6.4 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.

6.5 Mailing address

Blue Squirrel
686 E. 8400 South
Sandy, UT 84070

7 Reference

7.1 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.

ASMTP – 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.
ESMTP – Extensions to Simple Mail Transfer Protocol – A specification for additional

features beyond SMTP. See SMTP. ESMTP servers can support additional login methods.
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 trival for a human.

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.

7.2 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 "abababab".

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.
\0dd	0dd	An octal character code, where *dd* 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.

7.3 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)
```

7.4 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 -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- K -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- V -

- W -

- Y -