SpamSieve 2.7 Manual

C-Command Software
c-command.com

May 21, 2008

Contents

1   Introduction

1.1   What Is SpamSieve?

SpamSieve is a Macintosh application that filters out unsolicited mass mailings, commonly known as "spam." Previously, most people just ignored spam messages or created simple rules in their e-mail programs to filter them out. In recent years and months, the spam problem has gotten worse. Today's spam is harder to detect, and there is more of it.

SpamSieve gives you back your inbox by bringing powerful Bayesian spam filtering to Mac e-mail programs. It's quick and easy to control SpamSieve from within your mail program, and you can customize how it interacts with the rest of your message sorting rules.

SpamSieve learns what your spam looks like, so it can block nearly all of it. It looks at your address book and learns what your good messages look like, so it won't confuse them with spam. Other spam filters get worse over time as spammers adapt to their rules; SpamSieve actually gets better over time as *it* adapts its filtering to your mail.

SpamSieve doesn't delete any messages—it only moves them to a different folder in your e-mail program—so you'll never lose any mail. By learning from the very messages that *you* receive, SpamSieve is able to block nearly all of your spam, without putting your good messages in the spam mailbox. SpamSieve works with any number of mail accounts, of whatever types are supported by your e-mail software (e.g. POP, IMAP, Hotmail, AOL). You can even use it with multiple e-mail programs at the same time, for instance if you use one for work mail and one for personal mail.

1.2   Identifying Spam

SpamSieve uses a variety of methods to identify spam messages, but by far the the most important is a statistical technique known as *Bayesian analysis.* For a more in-depth treatment of this technique applied to spam, see this article by Paul Graham[1] and the papers it references. Bayesian spam filtering is highly accurate and adapts to new types of spam messages "in the field."

First, you *train* SpamSieve with examples of your good mail and your spam. When you receive a new message, SpamSieve looks at how often its words occur in spam messages vs. good messages. Lots of spammy words mean that the message is probably spam. However, the presence of words that are common in your normal e-mail but rare in spam messages can tip the scale the other way. This "fuzzy" approach allows SpamSieve to catch nearly every spam message yet produce very few false positives. (A *false positive* is a good message mistakenly identified as spam. Most users consider false positives to be much worse than *false negatives*—spam messages that the user has to see.)

Because you train SpamSieve with your own mail, you have full control. If SpamSieve makes a

---

[1]`http://www.paulgraham.com/spam.html`

mistake, you can train it with the message in question so that in the future it will do better. Further, since spammers don't have access to the messages you trained SpamSieve with, they have no way of knowing how to change their messages to get through. Whereas other spam filters become less effective as spammers figure out their rules, *SpamSieve becomes more effective over time* because it has a larger corpus of your messages to work from.

1.3   Integration

Separate from the issue of identifying spam messages is the issue of how to prevent you from having to deal with them. There are basically six kinds of anti-spam software for doing this:

Challenge-Response Systems

> This software requires people who send you mail to prove that they are human, and not an automated spam-sending program. After sending you a message, they get a reply asking them to complete a task that is easy for humans but hard for computers. Only then is the message passed on to you. This system is a nuisance for senders, delays your reception of the mail, and becomes impractical when sending messages to a group of people. Also, challenge response systems cannot deal with spoofed senders or legitimate messages that are sent by programs.

Server-Side Filters

> This software runs on mail servers and often filters out spam before you ever see it. This means that you do not have to download the spam messages that it catches. However, some spam messages may still get through, and, unless the filter is perfect, a few legitimate messages will not. These could be important messages, and you will never know that you lost them.

Server-Side Taggers

> This variant of server-side filters does not delete possible spam messages before you download them. Instead, you download every message and configure your e-mail program to move messages that were tagged by the filter into a separate spam folder. This eliminates the major disadvantage of server-side filters—lost messages—however this type of filter is generally not as accurate as the ones below, because it does not adapt to your own mail.

Client-Side Filters

> This software connects to your mail server to delete spam messages before your e-mail program can download them. This is a clunky approach: to catch all the spam messages, you have to run the program right before your regular e-mail program checks for mail. This is difficult to time properly if you check your mail often, and even so you may download some messages that weren't filtered. You will also download every good message twice. The anti-spam software may let you see the messages that it filtered out, so that you can verify that there were no false positives. However, you have to do this using its interface, not your e-mail program's (which is typically nicer). And if there was a false positive you then have to transfer it into your e-mail program so that you can file and reply to it.

Client-Side Proxies

This is like a client-side filter except that the proxy downloads messages once and stores them locally. The e-mail program then "downloads" the good messages from the proxy. This addresses the timing and double-download problems of client-side filters, but interaction with the filter is still awkward because it happens outside your e-mail program. In addition, you lose some control over the connections to the mail server and which messages are left on the server.

Client-Side Integrated

This category includes SpamSieve and Apple Mail's built-in spam filter. Suspected spam messages are moved to a separate folder, which you can quickly scan at your leisure to make sure there are no false positives. The e-mail program downloads messages directly from the mail server, thus avoiding the problems of client-side filters and proxies. You can train the anti-spam software to improve its accuracy from inside your e-mail program, and accuracy is higher than with server-side filters because the anti-spam software can learn from the messages that *you* receive. You can also control how the spam filter interacts with your regular mail sorting rules.

1.4 Main Features

- Powerful Bayesian spam filtering results in high accuracy and almost no false positives. It adapts to the mail that *you* receive to get even better with time. Some other e-mail programs include Bayesian filters, but SpamSieve is more accurate.

- Integrates with your e-mail program for a superior user experience. Plus, you get the same great filtering if you ever switch e-mail programs or use more than one at a time.

- Integrates with the Mac OS X Address Book (and also Eudora's and Entourage's address books) so that messages from friends and colleagues are never marked as spam.

- Automatically maintains a blocklist so that it can instantly adapt to spam messages sent from particular addresses, and catch 100% of them.

- Automatically maintains a whitelist to guarantee that messages from particular senders or mailing lists are never marked as spam, without cluttering your address book with these addresses.

- You can customize the whitelist and blocklist, adding sophisticated rules that match various message headers, or the message body. The rules can match text in a variety of ways, including using regular expressions.

- Can use the Habeas Safelist, which indicates messages that are not spam, as well as the "ADV" subject tag indicating that a message *is* spam.

- Many spammers encode the contents of their messages so that filters cannot see the incriminating words they contain. SpamSieve can decode and look inside these messages. Optionally it can mark them all as spam, on the theory that legitimate senders do not try to obscure their messages.

- SpamSieve keeps track of how accurate it is, how many good and spam messages you receive, and how these numbers change over time.

- Turn off new-mail notification in your e-mail program, and let SpamSieve notify you only when you receive non-spam messages.

- The corpus window and log let you see how each spam message was caught.

1.5   Why Choose SpamSieve?

Given that e-mail programs such as Apple Mail, Entourage, and Eudora include their own integrated spam filters, you may be wondering why you should consider SpamSieve. The answer is simple: SpamSieve's higher accuracy will save you time. You'll spend less time deleting spam messages from your inbox; in fact, SpamSieve gets rid of spam so effortlessly that you may even forget that you have it installed. Read what the press[2] and other SpamSieve users[3] have to say about it. Still not convinced? That's OK. You can try SpamSieve free for 30 days.

2   Installing and Updating

2.1   Requirements

SpamSieve is a universal binary that runs natively on both PowerPC- and Intel-based Macs using Mac OS X 10.4–10.5. It is designed to work with the following e-mail programs:

- Apple Mail[4] from Mac OS X 10.4 and later.

- Emailer[5] 2.0v3, previously available from Claris.

- Entourage[6] v.X (2001) and later (Entourage 2004 or 2008 recommended) from Microsoft.

- Eudora[7] 5.x or 6.x (in Sponsored or Paid mode) from Qualcomm. SpamSieve will also work with Eudora 8.0.0b1 (a.k.a. Penelope) if you follow the Thunderbird instructions. It does not work with Eudora 8.0.0b2 or 8.0.0b3.

- GyazMail[8] 1.2.0 and later (1.5.7 recommended).

- Mailsmith[9] 1.5 and later (2.1.5 or 2.2 recommended) from Bare Bones Software.

---

[2]http://c-command.com/spamsieve/press
[3]http://c-command.com/spamsieve/testimonials
[4]http://www.apple.com/macosx/features/mail/
[5]http://www.fogcity.com
[6]http://www.microsoft.com/mac/products/entourage2008/default.mspx
[7]http://www.eudora.com/email
[8]http://gyazsquare.com/gyazmail/
[9]http://www.barebones.com/products/mailsmith.html

- Outlook Express 5.0[10] and later from Microsoft.

- PowerMail[11] 4.0 and later (5.x recommended) from CTM Development.

- Thunderbird[12] 1.5.0.9 or 2.x from Mozilla, and Mac OS X 10.4 or later. SpamSieve does not work with Thunderbird 3 (which is in pre-release).

SpamSieve does not run on the iPhone, but you can use it together with your Mac to filter your iPhone mail. Just set both the Mac and the iPhone to access your mail account via IMAP. Whenever your Mac checks for new mail, SpamSieve will move the spam messages out of the IMAP inbox so that you don't see them on the iPhone.

SpamSieve works roughly the same way with each mail program. If you use multiple mail programs at once, SpamSieve will share its training data and statistics among them. Emailer, Eudora, and Thunderbird provide SpamSieve with access only to parts of each e-mail message, so SpamSieve's accuracy will be slightly reduced when using these mail programs, although it should still be much better than their built-in spam filters.

2.2 Updating From a Previous Version

SpamSieve will automatically read the corpus and statistics from previous versions. To update to the latest version of SpamSieve, quit your mail program and the SpamSieve application and then replace the old SpamSieve application file with the new one. That is, if SpamSieve is installed in the `Applications` folder, drag the new SpamSieve application icon into the `Applications` folder and click **Replace** when the Finder asks if you want to overwrite the old version. If you get an error saying that you do not have sufficient privileges, drag the old SpamSieve to the trash and empty it, and then drag the new one into the `Applications` folder. Then launch SpamSieve, followed by your mail program.

Mailsmith users should make sure that **Use SpamSieve** is still checked in Mailsmith's **Spam Handling** preferences.

2.3 Installing SpamSieve

Double-click the `SpamSieve-2.7.dmg` file to mount the SpamSieve disk image. Then drag the SpamSieve application to your `Applications` folder. It is important that SpamSieve be installed directly in the `Applications` folder (not in another folder, or in a subfolder), because otherwise your mail program might not be able to find it.

---

[10]`http://www.microsoft.com/mac/otherproducts/outlookexpress/outlookexpress.aspx?pid=outlookexpress`
[11]`http://www.ctmdev.com/powermail5`
[12]`http://www.mozilla.com/en-US/thunderbird/`
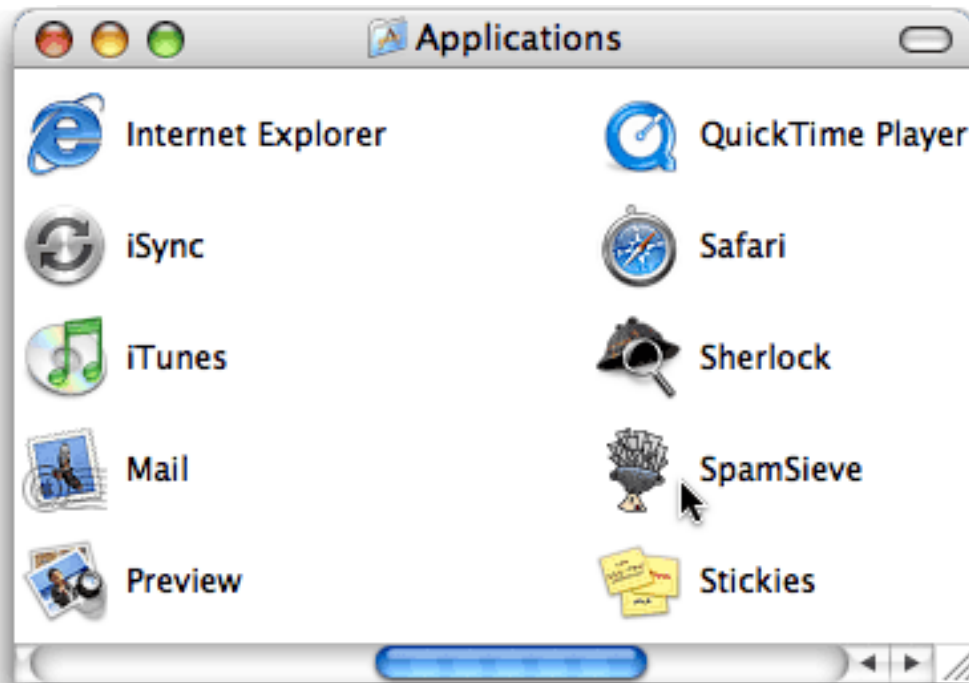
Next, you *must* follow the instructions for setting up SpamSieve to use it with your e-mail program. After setting up SpamSieve, you will need to train it with examples of your spam messages and good messages.

2.4   Uninstalling SpamSieve

To uninstall SpamSieve, delete any rules that you created for it in your e-mail program. You can also delete the AppleScripts and/or plug-in that you installed, and the SpamSieve application and its data files, which are stored in:

`/Users/<username>/Library/Application Support/SpamSieve`

The preferences file is stored in:

`/Users/<username>/Library/Preferences/com.c-command.SpamSieve.plist`

Apple Mail

The plug-in is located at:

`/Users/<username>/Library/Mail/Bundles/SpamSieve.mailbundle`

You can also re-enable Apple Mail's built-in junk mail filter from the **Junk Mail** tab of its **Preferences** window.

Emailer

The scripts are located in Emailer's `AppleScripts` folder (next to the Emailer application).

Entourage

The scripts are located in the `Entourage Script Menu Items` folder inside `Microsoft User Data` (which is probably in your `Documents` folder). Go to Entourage's **Tools** menu and select **Junk E-mail Protection** (or **Junk Mail Filter** in Entourage v.X) and re-enable Entourage's junk mail filter.

Eudora 6

The plug-in is located at:

`/Users/<username>/Library/Application Support/Eudora/PlugIns/SpamSieve Eudora Plug-In`

After uninstalling the SpamSieve plug-in, you can re-enable Eudora's own junk mail support by selecting the Eudora icon in the Finder and choosing **Get Info** from the **File** menu. In the **Plug-Ins** tab of the info window, you can check or uncheck the various plug-ins to enable or disable them. Check all the plug-ins containing the words "Junk" or "Spam."

Eudora 5

Delete the `SpamSieve Eudora Helper` file and also run the `Uninstall Eudora Helper` program that came with SpamSieve. (To access the uninstaller, choose **Show Other Scripts** from the **SpamSieve** menu.)

Outlook Express

The scripts are located in the `Script Menu Items` folder inside `Microsoft User Data` (which is probably in your `Documents` folder).

Thunderbird

Choose **Add-ons** (**Extensions** if you have Thunderbird 1.5) from Thunderbird's **Tools** menu. Select **SpamSieve Thunderbird Plug-in** in the list. Click the **Uninstall** button.

3   Using SpamSieve With Your E-Mail Client

Before you can use SpamSieve, you must give it some examples of messages you consider to be spam, and ones which you do not. You do this by selecting some messages and then telling SpamSieve whether they are spam or good. SpamSieve collects information from the messages it's trained with into its corpus, which it uses to predict whether subsequent messages are spam.

For the details of how to train SpamSieve, find the section below that corresponds to your e-mail program. For now, what's important is that you will train SpamSieve with both good messages and spam messages. Don't worry; it learns quickly!

First, you'll train SpamSieve with a batch of messages to get it started recognizing your mail. The **Corpus** section at the bottom of the Statistics window shows how many good and spam messages SpamSieve has been trained with, and what percentage of them are spam. After the initial training, SpamSieve will automatically train itself, and you'll only need to train it to correct mistakes.

For the initial training, use as many messages as you have on-hand, subject to two requirements:

Do not use more than 1,000 messages.

> Using up to 1,000 recent messages in the initial training lets SpamSieve start out with a high level of accuracy. In general, the more messages you train SpamSieve with, the better its accuracy will be. However, using more than 1,000 messages initially, would "fill up" SpamSieve's corpus with older messages, making it slower and less effective at adapting to new kinds of spam that you'll receive in the future.

The messages should be approximately 65% spam.

> This means 650 spams out of 1,000 messages, 325 out of 500, or 195 out of 300. For example, if you have 500 good messages but only 400 saved spam messages, don't train SpamSieve with those 900 messages. This would unbalance the corpus, making SpamSieve inaccurate and slower to learn. Instead, train it with the 400 spams and about 260 representative good messages. This will get it started at a higher level of accuracy. As new messages arrive, SpamSieve will automatically learn from them, keeping its corpus balanced, and its accuracy will improve.

Accuracy will improve with time, but if you've used at least 100 or so messages in the initial training, SpamSieve should immediately start moving *some* of the incoming spam messages to your spam folder. If you don't see results right away, check the setup in your mail program. After a few hundred messages of each type are in the corpus, SpamSieve should be catching most of your spam.

If SpamSieve marks a good message as spam, you should tell SpamSieve that it is a good message. This lets SpamSieve know that it made a mistake, and also adds the message to the corpus to improve future accuracy. Likewise, if SpamSieve marks a spam message as good, you should tell SpamSieve that it is a spam message (even if[13] you think the message might confuse SpamSieve). *If you do not correct SpamSieve when it makes mistakes, its accuracy will deteriorate over time.* Also, the *sooner* you correct SpamSieve, the better; by promptly correcting SpamSieve, you ensure that it's always acting on accurate information.

If you make a mistake and tell SpamSieve that a message is spam when it is actually good (or vice-versa), simply correct yourself as you would correct SpamSieve. That is, if the message is good,

---

[13]http://c-command.com/blog/2006/11/11/tell-spamsieve-the-truth/

train it as good; if it is spam, train it as spam. SpamSieve will "undo" the previous, incorrect, training.

3.1 Apple Mail

3.1.1 Installing

In addition to these written instructions, there is a video[14] that demonstrates how to set up and train SpamSieve with Apple Mail.

1. Quit Apple Mail. Then double-click the SpamSieve application and choose **Install Apple Mail Plug-In** from the **SpamSieve** menu at the top of the screen. When you open Mail once more, you should see three SpamSieve items in the **Message** menu:

2. Choose **New Mailbox**. . . (or **New**. . .) from Apple Mail's **Mailbox** menu, and create a new mailbox called **Spam** with location **On My Mac**. (The capitalization is important; do not call the mailbox **SPAM** or **spam**.)

3. Choose **Preferences**. . . from the **Mail** menu and click the **Rules** button in the toolbar. Click the **Add Rule** button. Change the description to **SpamSieve**. (The description of the rule *must* start with **SpamSieve**, but you can add additional text after that, if

---

[14]http://c-command.com/blog/2007/01/24/spamsieve-screencast/

you want.) Change the **From** menu to say **Message Type** (if you have Mac OS X 10.5) or **Every Message** (if you have Mac OS X 10.4). Then, next to **Move Message**, select the **Spam** mailbox that you just created. The rule should now look like:
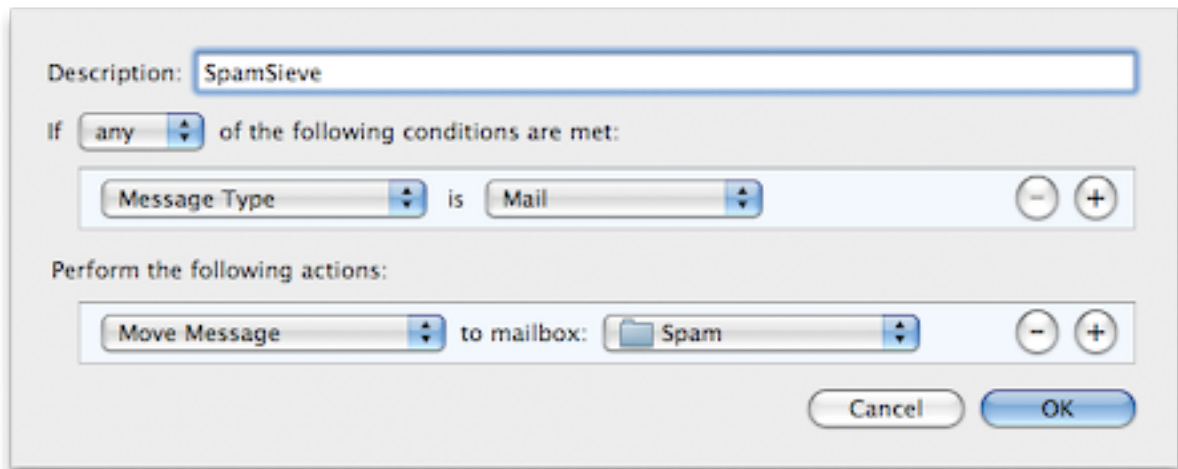
Please note that although the rule *looks* like it will move every message to the **Spam** mailbox, because you have installed SpamSieve's plug-in, it will only move the spam messages.

Now click **OK** to close the rule and save your changes. Apple Mail may ask if you want to apply the rule; click **Don't Apply** (or **No** if you have Mac OS X 10.4).

4. Drag the SpamSieve rule to the top of the list so that SpamSieve will be able to filter all of your mail.
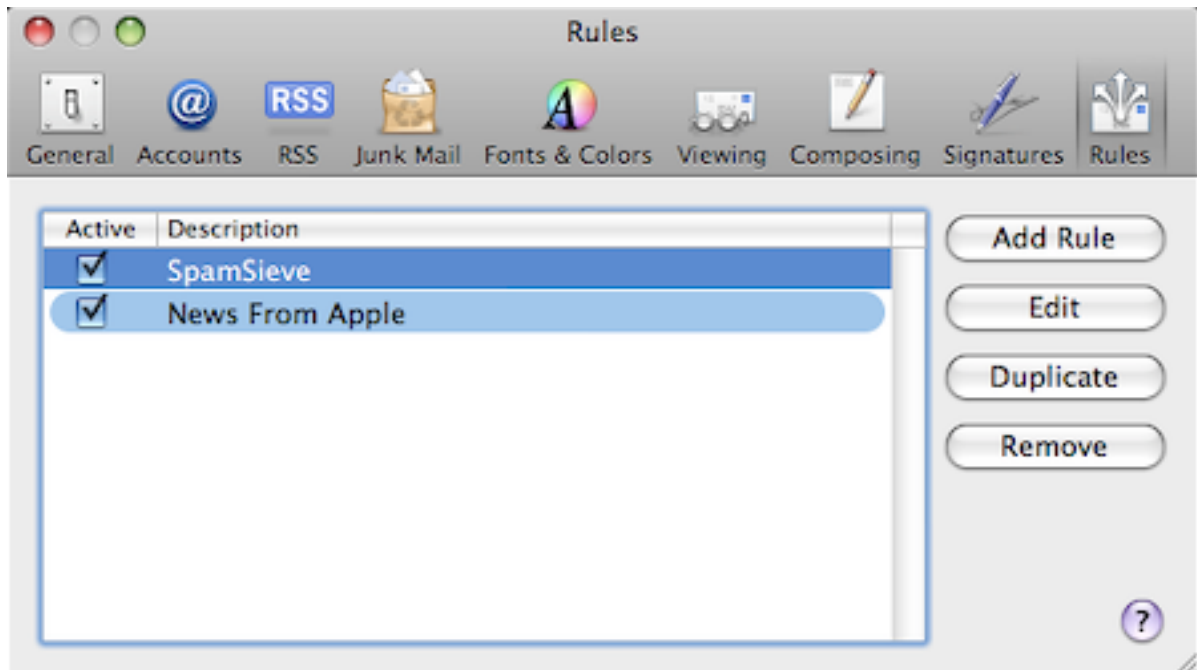
5. Delete any messages in the **Junk** mailbox. The spam messages will move to the **Trash** mailbox. (If you do not have a **Junk** mailbox you can skip this step.)

6. Go to the **Junk Mail** tab of Apple Mail's **Preferences** window and uncheck **Enable junk mail filtering**. This will hide Mail's **Junk** mailbox and disable its junk mail filter so that it doesn't interfere with SpamSieve.
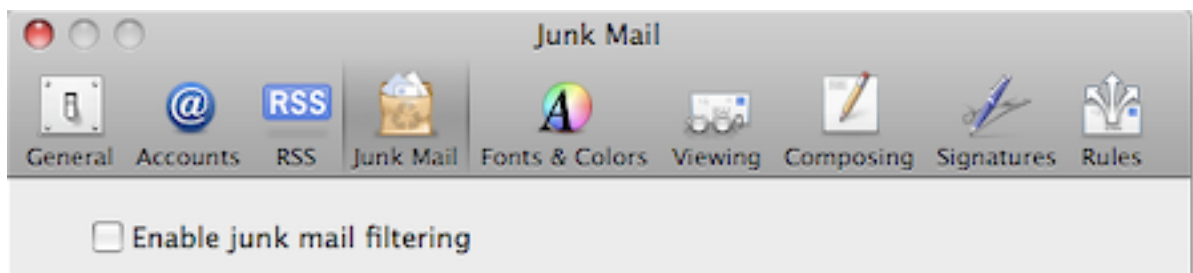
7. So that it starts off at a good accuracy level, you should now train SpamSieve with some examples of your good and spam messages. (There should be spam messages in the **Trash** from Step 5.) To train SpamSieve with some messages, select them in Apple Mail's message list, and then choose one of the **SpamSieve - Train as ___** commands from the **Message** menu.

SpamSieve will now automatically move new spam messages that you receive to the mailbox called **Spam**. If SpamSieve is not running when you receive new messages, it will launch automatically.

16

To further customize SpamSieve, you can use the SpamSieve - Change Settings command in Mail's **Message** menu or modify the rule. You can optionally turn off Mail's **New mail sound** in the **General** preferences and instead let SpamSieve notify you only when you receive new non-spam messages.

If you are using an iPhone, it is recommended that you set both Apple Mail and the iPhone to connect to your account via IMAP rather than POP. To do this, choose **IMAP** as the **Account Type** when setting up the account in Mail. This way, SpamSieve on your Mac will be able to filter the spam out of the inbox on the iPhone.

3.1.2 Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **SpamSieve - Train as Spam** from the **Message** menu. The messages will be colored in gray and moved to the **Spam** mailbox. To train SpamSieve with good messages, select one or more of them and then choose **SpamSieve - Train as Good** from the **Message** menu.

The keyboard shortcuts for these commands are Command-Control-S and Command-Control-G. You can change the keyboard shortcuts from the **Keyboard & Mouse** pane of System Preferences.
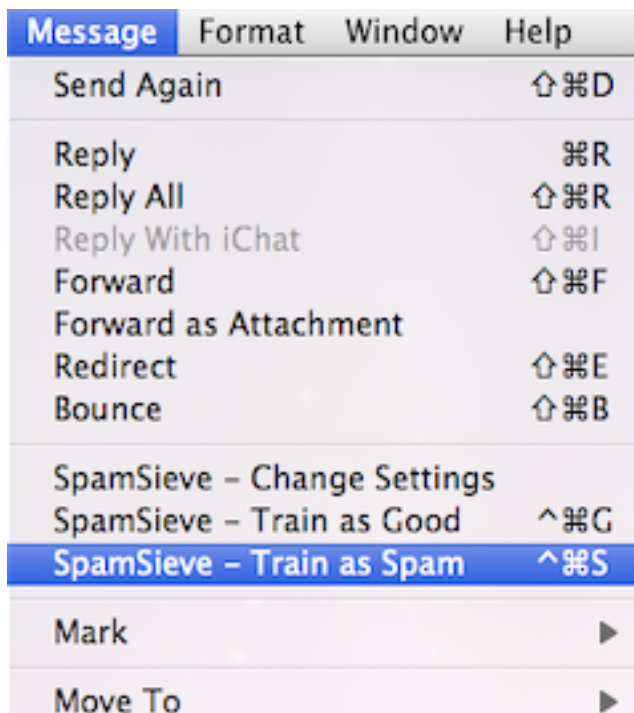
3.1.3   Manually Processing Messages

To manually ask SpamSieve to move messages that it thinks are spam to the **Spam** mailbox, select the messages and choose **Apply Rules** from the **Message** menu.

3.1.4   Spam Message Colors

SpamSieve sets the colors of spam messages to reflect how spammy it thinks they are. The most spammy messages are colored Blue. Less spammy messages are colored Gray, Purple, Red, Orange, or Yellow (in that order); good messages are left uncolored. The Change Settings command lets you enable or disable spam message coloring.

If you tell Mail to sort the **Spam** mailbox by color, the most spammy messages will be at the top, and the least spammy ones at the bottom. Thus, if you are skimming the **Spam** mailbox for false positives, you should spend more time examining the messages at the bottom.

You can also use rules in Mail to file messages into different mailboxes (or otherwise process them differently) based on how spammy they are.

- To move all spam messages to a single mailbox, create a single rule named **SpamSieve**, as shown here:
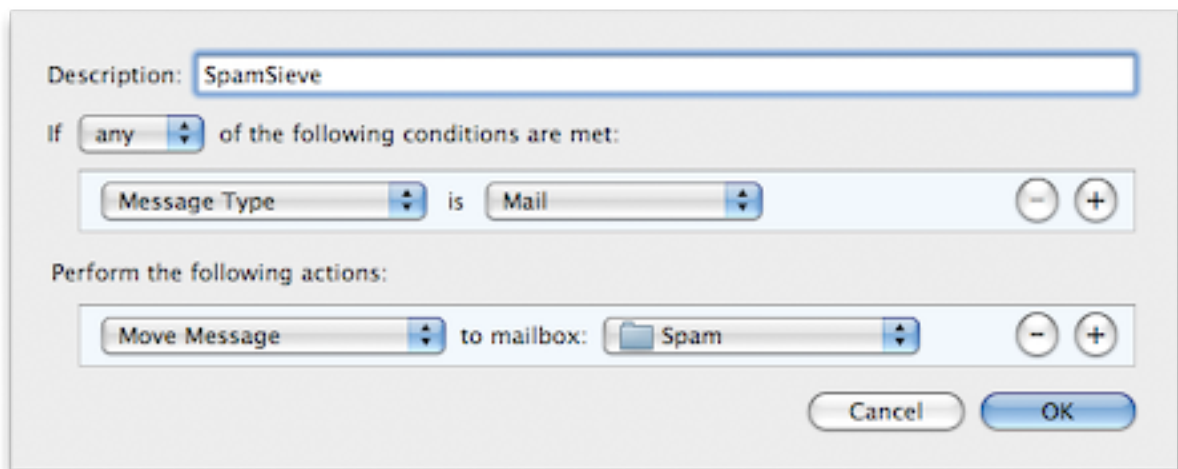
- To separate spam messages by color (spamminess), you should *instead* create two or more rules. The first rule should be named **SpamSieve [Score]**. As above, you probably want the conditions to be **Message Type is Mail** (or **Every Message** if you have Mac OS X 10.4). When this rule is applied, SpamSieve will calculate the spam score of the message and set its color accordingly. The actions of the [**Score**] rule will be ignored.

Below the [**Score**] rule you can create one or more rules that process messages based on their color. Each of these rules should have a name that starts with **SpamSieve**, followed by one or more color names in square brackets. Again, the rule conditions should be **Every Message**. For example, to make a rule that matches the most spammy Blue and Gray messages, you would name it **SpamSieve [Blue][Gray]** (or **SpamSieve [Gray][Blue]**). As a shorthand for listing *all* of the colors, you can simply write [**Spam**]. To match non-spam messages you can write [**White**]. You can include additional descriptive text after the brackets to remind you of what the rule does.

Example: To move blocklisted messages to the trash and other spam messages to the **Spam** mailbox, you would need three rules:

1. SpamSieve [Score] (calculates the spam score/color) / Message Type is Mail / Move Message to mailbox Spam
2. SpamSieve [Blue] (move very spammy messages to the trash) / Message Type is Mail / Move Message to mailbox Trash
3. SpamSieve [Spam] (move the remaining spam messages) / Message Type is Mail / Move Message to mailbox Trash

3.2 Emailer

3.2.1 Installing

1. Choose **Show Other Scripts** from SpamSieve's **SpamSieve** menu. Copy the files from the `For Emailer Users` folder into Emailer's `AppleScripts` folder:
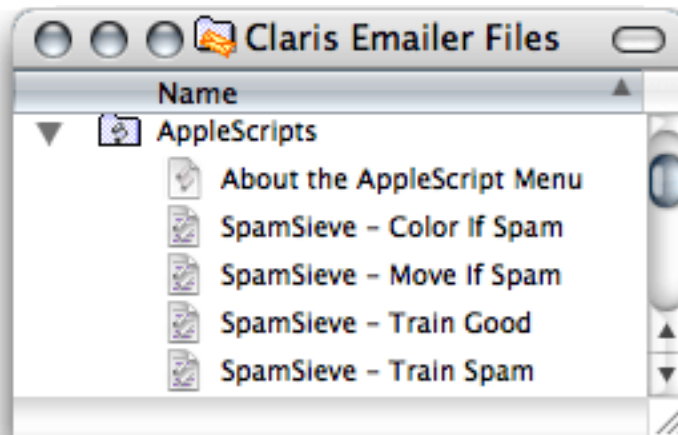
You may need to quit and re-launch Emailer in order for it to notice that you have installed the SpamSieve AppleScripts.

2. If you want SpamSieve to color messages that it thinks are spam, set up a mail action in Emailer that looks like this (using the **Define Actions. . .** button to set the "Run the AppleScript" action):

3. If, instead, you want SpamSieve to move suspected spam messages to a **Spam** folder (that it creates automatically), set up a mail action in Emailer that looks like this:

SpamSieve will now automatically color or move new spam messages that you receive, depending on which mail action you set up. If SpamSieve is not running when you receive new messages, it will launch automatically.

3.2.2   Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **SpamSieve - Train Spam** from Emailer's **Scripts** menu. To train SpamSieve with good messages, select one or more of them and then choose **SpamSieve - Train Good** from Emailer's **Scripts** menu.

3.2.3   Manually Processing Messages

To manually ask SpamSieve to color or move messages that it thinks are spam, select the messages and choose **SpamSieve - Color If Spam** or **SpamSieve - Move If Spam** from Emailer's **Scripts** menu.

3.3   Entourage

3.3.1   Installing

1. Go to Entourage's **Tools** menu and select **Junk E-mail Protection** (or **Junk Mail Filter** in Entourage v.X). Turn off Entourage's junk filter by clicking **None** and then **OK** (or uncheck **Enable Junk Mail Filter** in Entourage v.X).

2. Open the **Mailing List Manager**, also in the **Tools** menu, and see if there are any items listed there. If so, you can leave them for now, but if you find that SpamSieve isn't processing certain messages, you should either make sure that **Do not apply rules to list messages** is unchecked for each Mailing List Manager rule or you should try removing the rules from the Mailing List Manager. (You can re-create them as regular rules.)

3. Open Entourage's Preferences window. If you see an option in the **General Preferences** for **Sync Services**, select it and make sure that **Synchronize contacts with Address Book and .Mac** is checked. This will cause Entourage to sync its contacts[15] with the Mac OS X address book so that SpamSieve can access your addresses and know from the start that your regular contacts aren't spammers. You are now done with Step 3.

    If you don't see **Sync Services** (meaning that you have a version of Entourage prior to 11.2.3 or a version of Mac OS X prior to 10.4), then there are a few more things to do:

    - If you have Entourage 2004 or later, go to Entourage's **Security** preferences and make sure that **Warn before allowing an external application to access the address book** is unchecked. If there are no **Security** preferences in your version of Entourage, you can skip this step.

---

[15]http://www.entourage.mvps.org/faq_topic/sync_services_basics.html

- Double-click the SpamSieve application and choose **Preferences** from the **Spam-Sieve** menu. Make sure that **Use Entourage address book** is checked, and click the **Load** button. Then click on the SpamSieve icon in the Dock and choose **Update Address Book "Me" Card** from the SpamSieve menu (next to the Apple menu).

4. Choose **Install Entourage Scripts** from the **SpamSieve** menu. After you quit and re-launch Entourage, you should four SpamSieve items in Entourage's **Scripts** menu:
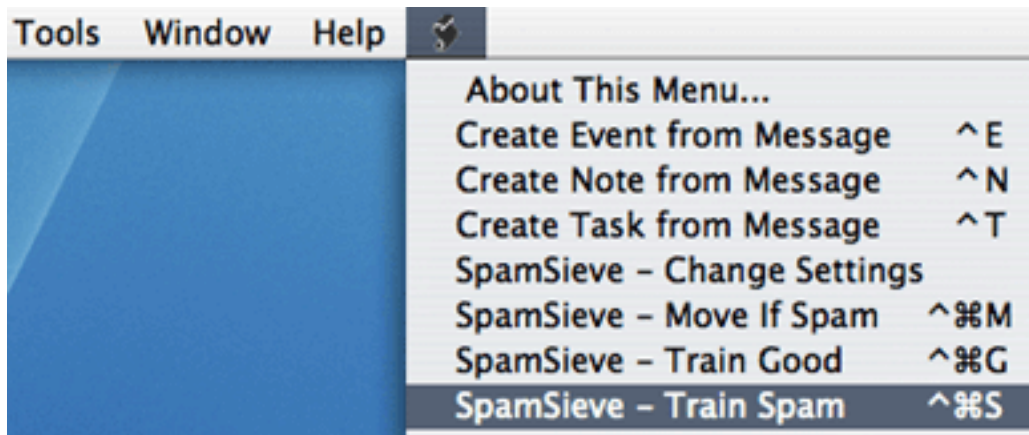
5. Now, set up a mail rule in Entourage that looks like this:
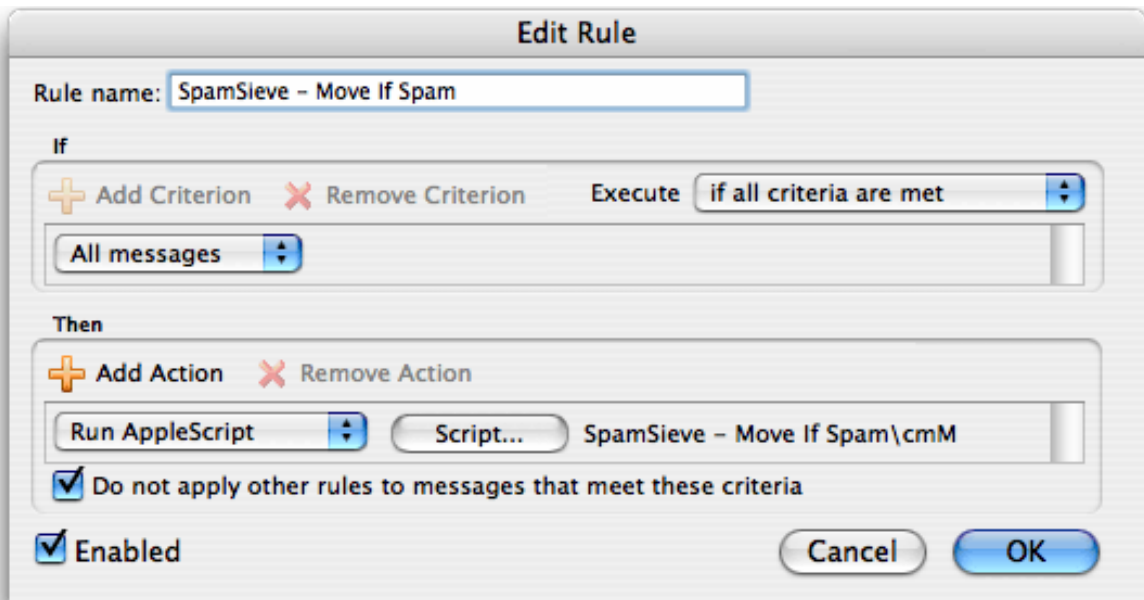
To do this, choose **Rules** from Entourage's **Tools** menu. Click on the tab corresponding to the type of account you have (e.g. POP). If you have more than one kind of account,

you will need to create an identical rule for each account type. Click the **New** button. Change the name of the rule to **SpamSieve - Move If Spam**. Then click just to the left of **Change status** to select the first action. Click **Remove Action** to delete the **Change status** action. Click on the menu that says **Set category** and select **Run AppleScript**. Then click the **Script**... button and **Select** the SpamSieve - Move If Spam\cmM file. This file is stored in the Entourage Script Menu Items folder:
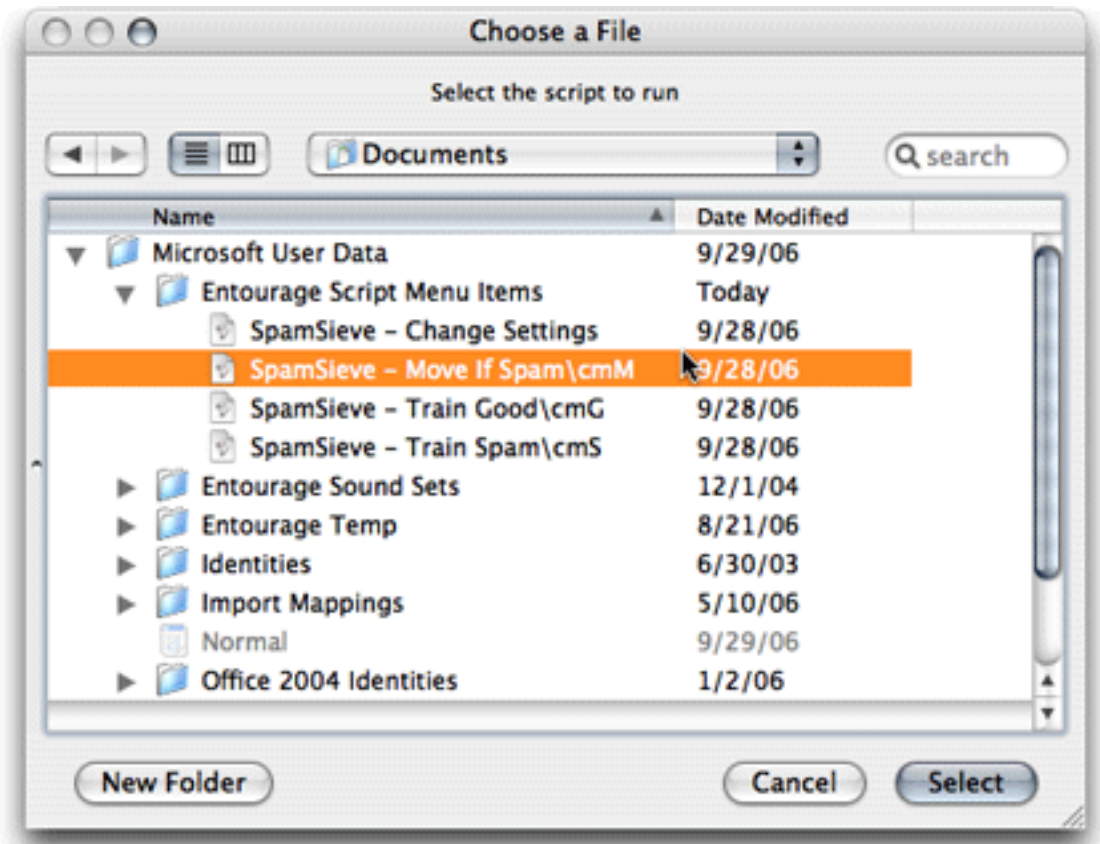
It is important that you create the rule exactly as shown. Do not add additional actions below the action that runs the AppleScript. Such actions would apply to all messages (not just spam ones), which is probably not what you want.

6. If you are using a POP account and have no other Entourage rules, you are now done. If you have Entourage rules to filter your non-spam messages, or if you are using an IMAP, Hotmail, or Exchange account, you will need to do a few more things. Drag the SpamSieve rule to the top of the list and then follow the instructions in Two SpamSieve Rules.

SpamSieve will now automatically move new spam messages that you receive to the **Junk E-mail** folder. If SpamSieve is not running when you receive new messages, it will launch automatically.

The following customizations are optional but recommended:

- Choose **Entourage ▷ Preferences**... and click on **Notification**. Turn off the sounds and new mail notifications, and let SpamSieve notify you only when you receive new non-spam messages.

- If you're using an IMAP account, choose **Tools ▷ Accounts**. Edit the account and click on the **Options** tab. Make sure that **Always download complete message bodies** is checked and that **Partially receive messages over** is not checked.

To further customize SpamSieve, you can use the Change Settings command in Entourage's **Scripts** menu.

3.3.2 Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **SpamSieve - Train Spam** from Entourage's **Scripts** menu. To train SpamSieve with good messages, select one or more of them and then choose **SpamSieve - Train Good** from Entourage's **Scripts** menu.
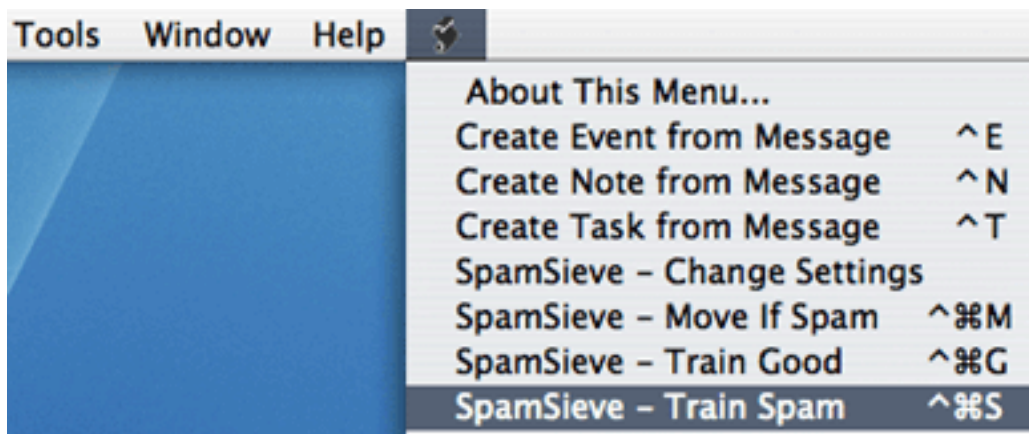
The keyboard shortcuts for these commands are Command-Control-S and Command-Control-G.

Note that due to the way Entourage's AppleScript interface works, you may not be able to train SpamSieve by selecting messages in mail views. Instead, select the messages in their actual folders. Also, the training commands do not move IMAP messages to/from the spam folder as they do POP messages.

Make sure that you correct SpamSieve's mistakes by using the commands in the **Scripts** menu—do not click the underlined blue text to indicate that a message is not spam.

3.3.3 Manually Processing Messages

To manually ask SpamSieve to move messages that it thinks are spam to the **Junk E-mail** folder, select the messages and choose **Apply Rule** ▷ **All Rules** from Entourage's **Message** menu.

3.3.4 Spam Message Categories

SpamSieve colors spam messages in Entourage using one of two categories. Messages that you mark as spam (using the **SpamSieve - Train Spam** command) and incoming messages that SpamSieve thinks are spam are colored with category **Junk**. Incoming messages that SpamSieve thinks are spam, but which it is less sure about, are colored with category **Uncertain Junk**. This makes it easier for you to check through the **Junk E-mail** folder for false positives.

It is also possible to have Entourage put the **Junk** and **Uncertain Junk** messages in separate folders. To do this, setup your SpamSieve rules in Entourage as shown here. Create a new folder in Entourage called **Uncertain Junk**. Then create a third rule called **SpamSieve - Move Uncertain Messages** that looks like **SpamSieve - Move Messages**, except set it to match category **Uncertain Junk** and choose the **Uncertain Junk** folder for it to move the messages to.

You can adjust the threshold for uncertainty in SpamSieve's preferences. For example, if you want SpamSieve to put blocklisted messages in the trash and other spam messages in the **Junk E-mail** folder, you would set the threshold to 98. Then set **SpamSieve - Move Messages** to put messages in the **Deleted Items** folder, and set **SpamSieve - Move Uncertain Messages** to put messages in the **Junk E-mail** folder.

To turn off the uncertain spam feature, so that all spam messages are marked using the **Junk** category, use the Change Settings command.

3.3.5 Two SpamSieve Rules

This section, for Entourage 2004 and 2008 users, describes how to setup Entourage rules for SpamSieve if:

- you are using an IMAP, Hotmail, or Exchange account, or

- you want to filter non-spam messages with additional Entourage rules, after they've been processed by SpamSieve

At this point, you should have followed the instructions in the previous section to create an Entourage rule for SpamSieve. Uncheck the **Do not apply other rules**. . . option for the rule so that it looks like this:
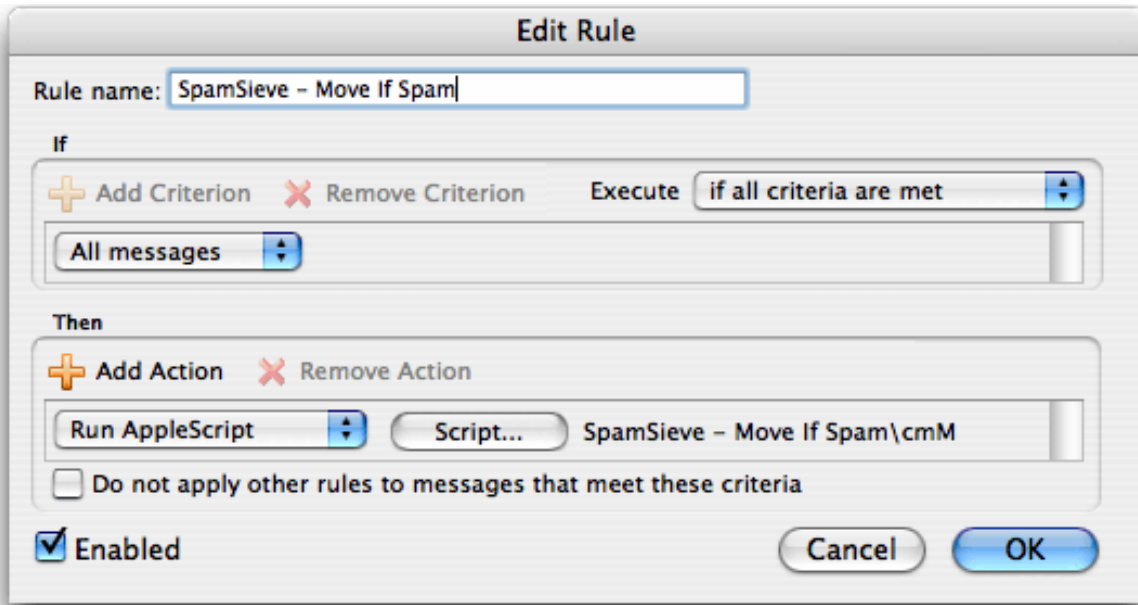
Then, create a second rule that looks like:
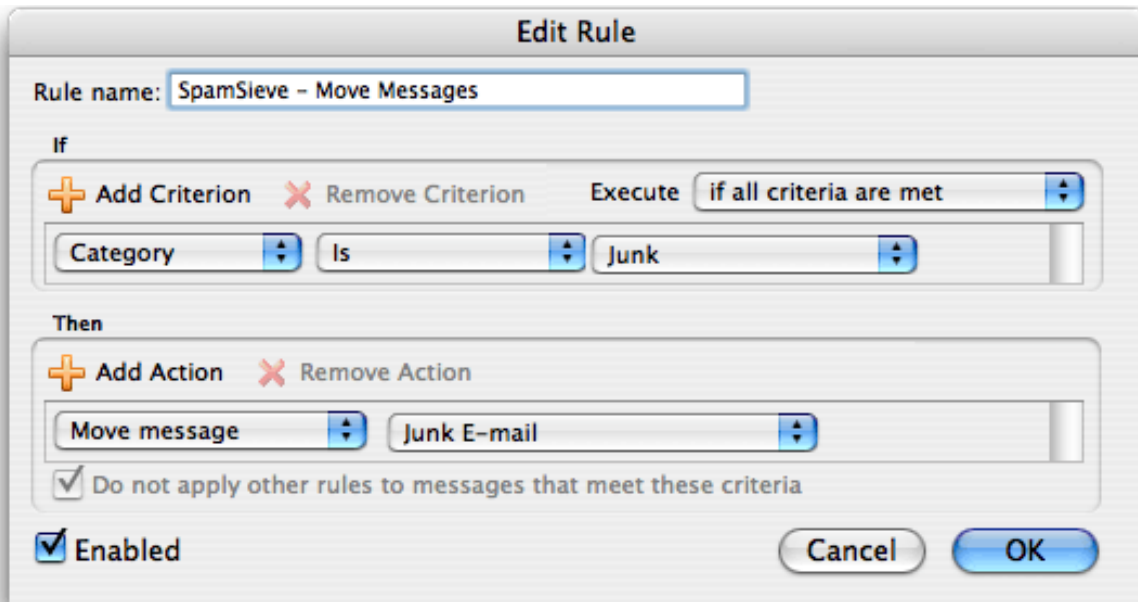
The action of the rule should be to move the messages to the **Junk E-mail** folder. After setting up the rule, make sure that the **SpamSieve - Move Messages** rule appears directly *below* the **SpamSieve - Move If Spam** rule in Entourage's **Rules** window. Any additional rules that you

want to process the non-spam messages should be listed below the **SpamSieve - Move Messages** rule.

Note: If you are using Gmail and IMAP with Entourage, change the criterion for the "SpamSieve - Move If Spam" rule from "All messages" to "Folder Is Inbox (Gmail)."

3.3.6   IMAP Accounts and Entourage v.X

Entourage v.X does not support moving IMAP (or Hotmail or Exchange) messages via AppleScript. Thus, if you have one of these types of accounts, the spam messages will not be moved to your **Junk E-mail** folder. The best solution is to update to Entourage 2004 or 2008, which do not have this limitation. If you do not wish to do this, here are some possible workarounds:

- If you do not require IMAP, you can try creating a POP account in Entourage and re-entering your account information. Many IMAP accounts also work via POP, and this will allow SpamSieve to move the messages that it thinks are spam.

- Create an Entourage rule that moves messages that SpamSieve has marked as junk into another folder. After receiving mail, manually apply this rule to the messages in your IMAP account.

- Make a mail view of your IMAP account that looks for messages that are not junk. In this way, you can view your good messages without being distracted by the spam ones.

3.4   Eudora 6

3.4.1   Installing

If you are using Eudora 5.2 or Eudora 6 Lite, please see the Eudora 5.2 section.

1. Double-click the SpamSieve application and choose **Install Eudora Plug-In** from the **SpamSieve** menu. SpamSieve will install its plug-in, disable other junk mail plug-ins (which would conflict with SpamSieve), and reveal the Eudora application file for you.

2. Select the Eudora application file and choose **Get Info** from the Finder's **File** menu. Expand the **Plug-ins** pane, and check the **Esoteric Settings** plug-in to enable it. Make sure that **SpamWatch OSX** and **SpamHeaders OSX** are unchecked. You can now close the info window and launch Eudora.

When you start up Eudora, you should see SpamSieve listed in the **About Message**

Plug-ins. . . window that is accessible from the **Eudora** menu. Please note that the version number displayed in this window is the version of the SpamSieve Eudora Plug-In; it will not be the same as the version number of the SpamSieve application. The current plug-in version is displayed in SpamSieve's about box.

3. Choose **Preferences**. . . from the **Eudora** menu, scroll down to the **Junk Extras** settings panel (which is at the very bottom), and check **Always enable Junk/Not Junk menu items**. Next, select the **Junk Mail** pane and make sure that **Hold junk in Junk mailbox** is checked. The **Junk Threshold** slider *must* be set to the middle position (50). If you are using IMAP, make sure that **Run junk scoring plugins on this IMAP account** is checked in the **IMAP** settings pane.

Now Eudora will use SpamSieve to filter all incoming messages. It will move the spam messages to the **Junk** mailbox. This happens *before* Eudora runs any incoming message filters that you have set up.

Normally, Eudora will launch the SpamSieve application when new messages arrive or when you train SpamSieve from inside Eudora. If this does not happen, make sure that the SpamSieve application is stored directly in your applications folder.

3.4.2   Training SpamSieve

To train SpamSieve to recognize your spam, select one or more spam messages (in any mailbox) and then choose **Junk** from Eudora's **Message** menu.

To train SpamSieve to recognize your good mail, select one or more non-spam messages (in any mailbox) and then choose **Not Junk** from Eudora's **Message** menu.

You can also use toolbar buttons[16] for training SpamSieve.

3.4.3   Manually Processing Messages

It is not possible to manually process selected Eudora 6 messages with SpamSieve. Incoming messages will be processed automatically, however.

3.4.4   Setting Options

Eudora applies SpamSieve to all incoming messages. The **Junk Mail** area of Eudora's preferences lets you customize how Eudora interacts with SpamSieve. Note that the **Junk Threshold** slider will have no effect because SpamSieve always considers messages with scores of 50 or above to be

---

[16]http://www.eudora.com/email/features/spamwatch_mac_buttons.html

spam. Thus, you should set Eudora's junk threshold to 50 and use the slider in the **Advanced** tab of SpamSieve's preferences if you need to adjust its sensitivity.

Other settings in the **Junk Mail** pane do affect SpamSieve. For instance, if you check **Mail isn't junk if the sender is in an address book**, then Eudora will not pass those messages along to SpamSieve; it will assume that they are good. Note that Eudora always considers your address to be in its address book, even though it may not be explicitly listed there. Thus, if you receive spam that is forged so that it appears to be sent from your own address, you must uncheck **Mail isn't junk if the sender is in an address book** in order for SpamSieve to catch it.

To still have SpamSieve whitelist your address book, you can export[17] the Eudora address book to vCard and then import it into the Mac OS X Address Book, or use SpamSieve's Import Addresses... command to import the `Eudora Nicknames` file.

The **Junk Extras** area of Eudora's preferences lets you control some additional settings, such as whether junk messages are removed from the mail server.

3.4.5 Updating Eudora

Re-installing the Eudora application or updating it to a newer version may have the side effect of enabling Eudora's built-in junk mail filter plug-ins, which would interfere with SpamSieve. The next time you launch SpamSieve, it should detect this situation and disable the plug-ins automatically.

3.4.6 Installing the Plug-In Manually

If the **Install Eudora Plug-In** command doesn't work, you can install the plug-in manually as follows:

1. Go to the **SpamSieve** menu and choose **Show Other Scripts**.

2. In the Finder window that opens, hold down the Apple key and press Up Arrow. Now you should see a window containing the file `SpamSieve Eudora Plug-In`.

3. Create the folder:

   `/Users/<username>/Library/Application Support/Eudora/PlugIns/`

   and drag the `SpamSieve Eudora Plug-In` file into it.

---

[17]`http://homepage.mac.com/aamann/Eudora_vCard_Export.html`

3.5   Eudora 5.2

3.5.1   Installing

Using SpamSieve with Eudora 6 is highly recommended. However, SpamSieve can also work with Eudora 5.2, and some Eudora 6 users may prefer the configuration described here because it is more customizable.

1. Choose **Show Other Scripts** from SpamSieve's **SpamSieve** menu. Move the `SpamSieve Eudora Helper` file in the `For Eudora 5.2 Users` folder to the `Applications` folder of your hard disk. You will need to launch this applet the first time you use SpamSieve with Eudora.

   Also in the `For Eudora 5.2 Users` folder is the `Uninstall Eudora Helper` file. Run this applet if you no longer want to use SpamSieve with Eudora.

2. Create a mailbox in Eudora called **Spam** that is at the same level as the **In** mailbox. When you receive new spam messages, SpamSieve will move them to the **Spam** mailbox. It will also mark good messages by setting their priority to lowest (indicated by two downward pointing carets) and mark spam messages by setting their status to transfer error (indicated by a red "X").

3.5.2   Training SpamSieve

To train SpamSieve with spam messages, select one or more of them. Choose the **Filter Messages** command in Eudora's **Special** menu. Then double-click **Train Spam**.

To train SpamSieve with good messages, select one or more of them. Choose the **Filter Messages** command from Eudora's **Special** menu. Then double-click **Train Good**.

3.5.3 Manually Processing Messages

To manually ask SpamSieve to mark or move messages that it thinks are spam, select one or more of them. Choose the **Filter Messages** command in Eudora's **Special** menu. Then double-click **Filter**.

3.5.4 Setting Options

By configuring the `SpamSieve Eudora Helper` applet, you can tell SpamSieve to process your good messages and spam messages in other ways. First, quit the applet. Then open it using the Script Editor program in the `AppleScript` folder of your `Applications` folder. The top of the script contains the following lines:

```
property moveToSpamFolder      : true  -- moves spams to a "Spam" mailbox
property markSpamMessages       : true  -- marks spams with red x
property markSpamMessagesRead : false -- marks spams as "already read"
property labelSpamMessages     : false -- colors spam messages brown
property markGoodMessages       : true  -- marks good messages with carets
property labelGoodMessages      : false -- colors good messages green
property removeSpamMessagesFromServer : false
```

You can change a `false` to `true` or a `true` to `false` to set the options the way you want. For instance, to have SpamSieve not move spam messages into a separate mailbox, change the `true` in the first line to `false`. When you are finished making changes, choose **Save** in Script Editor's **File** menu, close the window, and then re-launch the SpamSieve Eudora Helper.

Script Editor 2.0 cannot edit the `SpamSieve Eudora Helper` applet. To customize the applet, use Script Editor 1.9 or a third-party script editor.

3.5.5 Eudora Limitations

The following limitations are due to problems with Eudora's "notification" interface. Because of these limitations it is recommended that you use Eudora 6 and the `SpamSieve Eudora Plug-In`, as described in the Eudora 6 section. The plug-in avoids these limitations.

- Eudora gives messages to SpamSieve *after* all the other filters have run. It is not possible to change this ordering.

- SpamSieve cannot filter messages that are moved by other filters. For instance, if you have a filter that moves incoming messages from Steve Jobs to a separate mailbox, SpamSieve will not mark any of those messages as spam, even if a spammer pretends to be Jobs. This

limitation applies to both automatic filtering of incoming mail and manual filtering of selected messages.

- Sometimes the wrong message is marked. That is, SpamSieve may decide that message A is spam and ask Eudora to mark it with a red "X"; in rare circumstances, Eudora will instead mark some other message B with the "X." You can tell if this has happened by comparing SpamSieve's log to the way the messages are marked in Eudora. This problem seems to occur when the **In** mailbox is sorted.

- Sometimes SpamSieve never sees a message that should have been filtered. You can tell if this has happened by the absence of that message in the log. It may help to remove any "notify user" filter action that you have set up.

- Sometimes SpamSieve determines that a message is good or spam, but Eudora does not mark it at all. You can tell if this has happened by comparing SpamSieve's log to the way the messages are marked in Eudora.

- SpamSieve cannot add or filter messages that are stored in the Trash mailbox or in mailbox files outside the `Mail Folder` folder in the `Eudora Folder`. Note that this includes all IMAP messages. To access these messages, first move them to a non-trash mailbox file that is stored inside the `Mail Folder` folder.

- If you manually apply filters while Eudora is in the process of downloading mail, Eudora will show the SpamSieve dialog box twice. If this happens, just choose **Skip** the second time.

- Sometimes Eudora erroneously shows the SpamSieve dialog when you check for new mail.

- Sometimes after a long delay in talking to the mail server, Eudora stops notifying SpamSieve when it receives new messages. You can work around this by quitting and re-launching the SpamSieve Eudora Helper.

3.6 GyazMail

3.6.1 Installing

To enable SpamSieve, open GyazMail's **Preferences** window and click **Junk Filter**. Make sure that **Enable Junk filtering** is checked and that the pop-up menu says **SpamSieve**.

By default, GyazMail will color the spam messages brown. If you want the spam messages to also be put in a separate folder, create a folder called **Spam**. Then click on **Rules** in the **Preferences** window and create a new rule as shown:
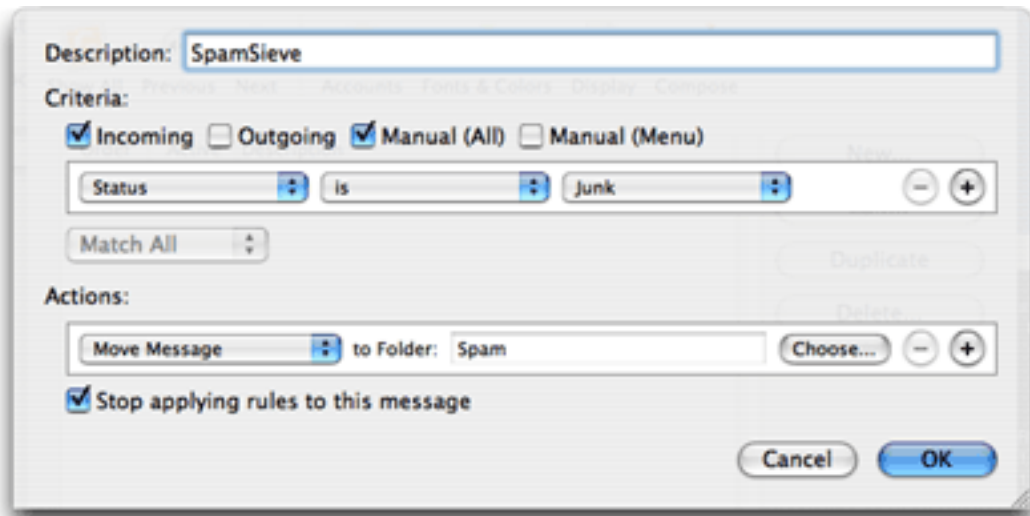
3.6.2 Training SpamSieve

To train SpamSieve with spam messages, select the messages, go to GyazMail's **Message** menu, and choose **Junk ▷ Mark as Junk**. This will make the **Message ▷ Status ▷ Junk** item checked.

To train SpamSieve with good messages, select the messages, go to GyazMail's **Message** menu, and choose **Junk ▷ Mark as Not Junk**. This will make the **Message ▷ Status ▷ Junk** item unchecked.

You can also use the **Junk** button on the toolbar or the **Message ▷ Status ▷ Junk** menu command to toggle the junk status of the selected messages.

3.6.3 Manually Processing Messages

To manually ask SpamSieve whether the selected messages are spam, choose **Junk ▷ Recheck Junk Status** from the **Message** menu.

3.7 Mailsmith

3.7.1 Installing

Mailsmith 2.0 and later feature direct integration with SpamSieve. This is more convenient and easier to use than the script- and filter-based integration that was necessary when using previous versions of Mailsmith. You can enable SpamSieve simply by clicking the **Use SpamSieve** checkbox in the **Spam Handling** pane of Mailsmith's preferences. For more information about using

SpamSieve with Mailsmith, please see Chapter 8 of the Mailsmith User Manual.

3.7.2   Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **Mark as Spam** from Mailsmith's **Message** menu. To train SpamSieve with good messages, select one or more of them and then choose **Mark as Non-Spam** from Mailsmith's **Message** menu.

3.7.3   Identifying Spam Messages

When using SpamSieve with Mailsmith, Mailsmith tags messages using the **Is Spam** and **Is Not Spam** properties. Although you can use Mailsmith's **Advanced Query** feature to search on these properties, they are otherwise not visible in the user interface. Therefore, you should mark spam messages in a visible way, either by letting Mailsmith move them to a separate mailbox, or by setting up a filter to change the messages' labels based on their **Is Spam** and **Is Not Spam** properties. Otherwise, you will not be able to correct SpamSieve's mistakes to improve its accuracy.

In Mailsmith 2.2 (in public beta as of this writing), this is no longer a concern because Mailsmith automatically marks each message with its spam score, from 0 to 100.

3.7.4   Mailsmith Extras

Choose **Show Other Scripts** from SpamSieve's **SpamSieve** menu. This reveals the `Mailsmith Extras` folder, which contains AppleScripts for use with Mailsmith. These make it possible for scripters to further customize and automate the labeling and marking of messages in Mailsmith. If you are using Mailsmith 2.0 and do not write your own AppleScripts, you can ignore the `Mailsmith Extras` folder.

You can add the AppleScripts to Mailsmith's **Scripts** menu by copying them to the `Scripts` folder inside the `Mailsmith Support` folder. A filter such as the following may be used to change the labels of incoming spam messages.
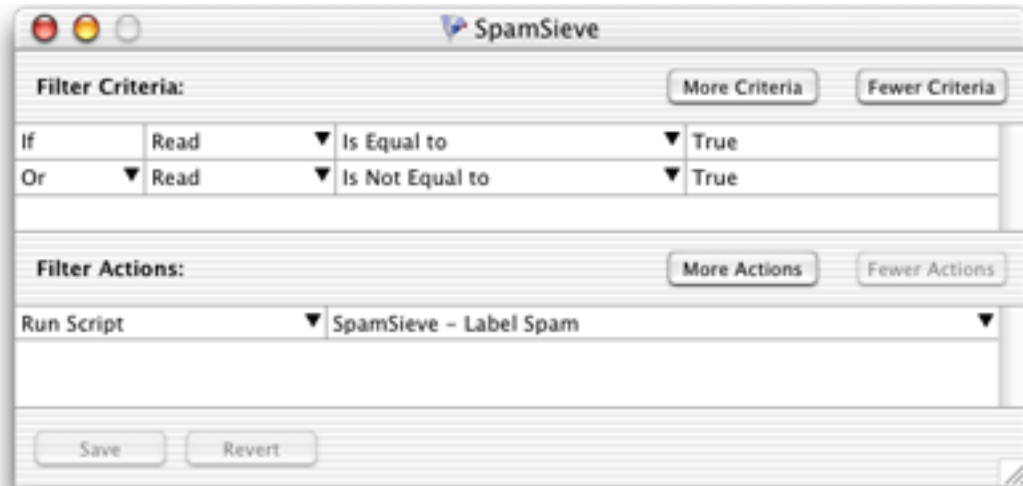
This filter will pass all messages along to SpamSieve for analysis. It will set the **Is Spam** or **Is Not Spam** property of the message, and change the label of the message if it is spam. This is roughly equivalent to enabling SpamSieve in Mailsmith's preferences, but because it uses AppleScript it is more customizable. Additionally, you can change the filter criteria to pass only select messages along to SpamSieve.

3.8   Outlook Express

3.8.1   Installing

1. Choose **Show Other Scripts** from SpamSieve's **SpamSieve** menu. Copy the files from the `For Outlook Express 5 Users` folder to the `Script Menu Items` folder inside the `Microsoft User Data` folder (which is likely in your `Documents` folder).

2. Follow the instructions for Entourage to create a rule in Outlook Express that applies the `SpamSieve - Move If Spam` script. SpamSieve will now move new spam messages that you receive to the **Spam** folder. If SpamSieve is not running when you receive new messages, it will launch automatically.

3.8.2   Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **Spam-Sieve - Train Spam** from Outlook Express's **Scripts** menu. To train SpamSieve with good messages, select one or more of them and then choose **SpamSieve - Train Good** from Outlook Express's **Scripts** menu. The keyboard shortcuts for these commands are Command-Control-S and Command-Control-G.

Make sure that you correct SpamSieve's mistakes by using the commands in the **Scripts** menu—do not click the underlined blue text to indicate that a message is not spam.

3.8.3 Manually Processing Messages

To manually ask SpamSieve to move messages that it thinks are spam, select the messages and choose **SpamSieve - Move If Spam** from Outlook Express's **Scripts** menu.

3.9 PowerMail 5

3.9.1 Installing

If you are using PowerMail 4, please see the PowerMail 4 section.

PowerMail 5 ships with built-in support for SpamSieve. To enable it, go to the **Mark as Spam** pane of PowerMail's **Preferences** window. Click the **Spam filter assistant**. . . button and tell the assistant that you want to use SpamSieve. For more information about how to configure PowerMail's handling of spam messages, please see the PowerMail documentation.

3.9.2 Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **Mark as Spam** from the **Mail** menu. To train SpamSieve with good messages, select one or more of them and then choose **Mark as Good** from the **Mail** menu.

3.10 PowerMail 4

3.10.1 Installing

1. Choose **Show Other Scripts** from SpamSieve's **SpamSieve** menu. Copy the files from the `For PowerMail 4.x Users` folder to the `PowerMail Scripts` folder inside the `PowerMail Files` folder. The `PowerMail Files` folder is probably located in your `Documents` folder.
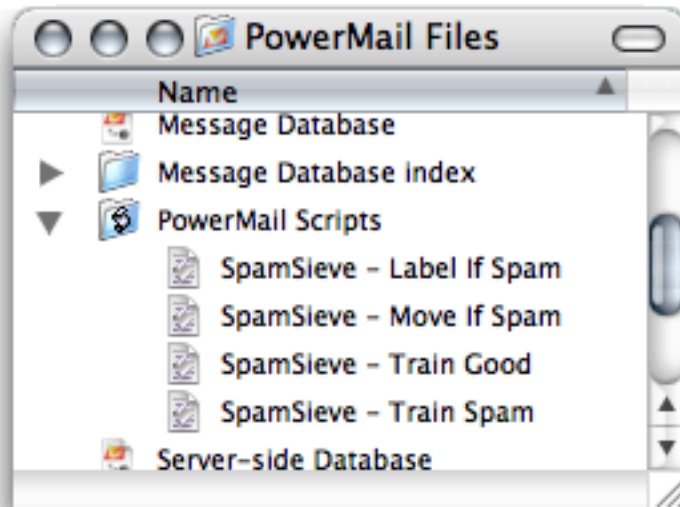
2. If you want SpamSieve to label messages that it thinks are spam, set up a filter in PowerMail that looks like this:
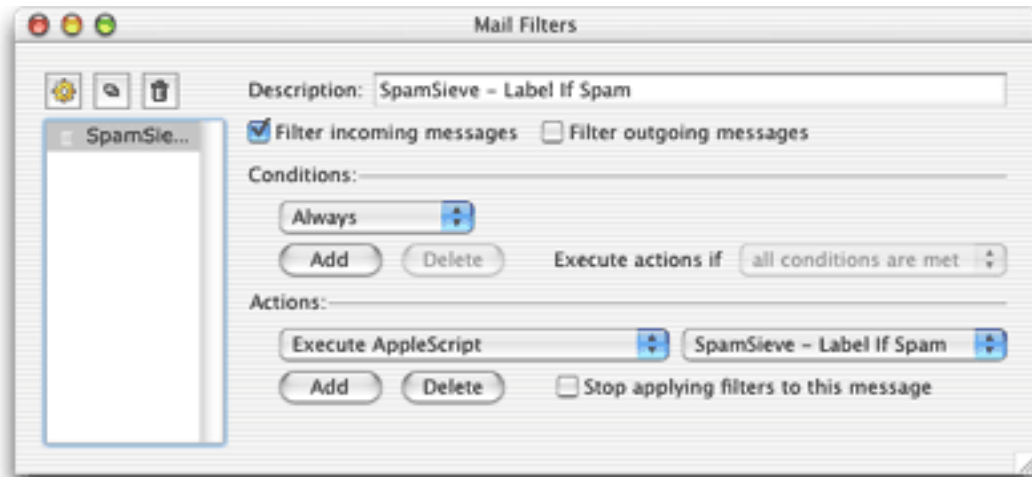
3. If, instead, you want SpamSieve to move suspected spam messages to a **Spam** folder (that it creates automatically), set up the filter to use the `SpamSieve - Move If Spam` script instead.

SpamSieve will now mark or move new spam messages that you receive. If SpamSieve is not running when you receive new messages, it will launch automatically.

3.10.2   Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **SpamSieve - Train Spam** from PowerMail's **Scripts** menu. To train SpamSieve with good messages, select one or more of them and then choose **SpamSieve - Train Good** from PowerMail's **Scripts** menu.

3.10.3   Manually Processing Messages

To manually ask SpamSieve to label or move messages that it thinks are spam, select the messages and choose **SpamSieve - Label If Spam** or **SpamSieve - Move If Spam** from PowerMail's **Scripts** menu.

3.10.4   IMAP Accounts

PowerMail does not support moving IMAP messages via AppleScript. Thus, if you use IMAP the **SpamSieve - Move If Spam** script will not move spam messages into your **Spam** folder. IMAP users should create the rule that uses the labeling script.

3.11   Thunderbird

3.11.1   Installing

1. Choose **Install Thunderbird Plug-In** from SpamSieve's **SpamSieve** menu.

2. Launch Thunderbird. Choose **Add-ons** (or **Extensions** if you have Thunderbird 1.5) from the **Tools** menu.

3. Click the **Install** button in the window that just opened. Thunderbird will ask you to select a file.

4. Click on **Desktop**, select the `SpamSieve Thunderbird Plug-In.xpi` file, and click Open.

5. Click the **Install now** button.

6. Quit Thunderbird and re-launch it. If you now go to the **Tools** menu and choose **Add-ons** (**Extensions** if you have Thunderbird 1.5) you should see the **SpamSieve Thunderbird Plug-In** listed there. Next to it will be the version of the plug-in. The current plug-in version is always listed at the bottom of SpamSieve's about box. You can now delete the `SpamSieve Thunderbird Plug-In.xpi` file from your desktop.

7. Do this step only if you have Thunderbird 1.5. Choose **Junk Mail Controls** from the **Tools** menu. You can now configure the junk filtering settings for your different accounts. On the **Settings** tab, make sure that:

- **Trust junk mail headers set by** is unchecked.
- **Move incoming messages determined to be junk mail to** is checked.
- **When I manually mark messages as junk** is checked.
- **When displaying HTML messages marked as junk, sanitize the HTML** is checked.

On the **Adaptive Filter** tab, make sure that **Enable adaptive junk mail detection** is checked.

8. Do this step only if you have Thunderbird 2.x. Choose **Account Settings** from the **Tools** menu. For each of your accounts in the list at the left (plus "Local Folders"), click on **Junk Settings** and make sure that:

- **Enable adaptive junk mail controls for this account** is checked.
- **Trust junk mail headers set by** is unchecked.
- **Move new junk messages to** is checked.

SpamSieve will now automatically filter your incoming mail.

3.11.2   Training SpamSieve

To train SpamSieve with spam messages, select one or more of them and then choose **Message ▷ Mark ▷ As Junk** or click the **Junk** button in the toolbar. To train SpamSieve with good messages, select one or more of them and then choose **Message ▷ Mark ▷ As Not Junk** or click the **Not Junk** button in the toolbar.

3.11.3   Manually Processing Messages

To manually ask SpamSieve to determine whether some messages are spam, select the messages and choose **Message ▷ Mark ▷ Run Junk Mail Controls**.

4   E-Mail Client Customization

SpamSieve works with your e-mail program to filter out spam messages. First, the mail program downloads new messages from the mail server. It then passes the messages to a plug-in or Apple-Script, which in turn passes them to the SpamSieve application. SpamSieve analyzes the messages to see whether they are spam. It returns the verdict to the plug-in or script, which then directs the mail program to move the messages to another folder.

4.1 Rule Ordering

Some of the e-mail programs that SpamSieve supports let you control the order in which the rules (a.k.a. filters or mail actions) that you have created process mail. How you order the SpamSieve rule is up to you. If you get a lot of spam that matches the rules you use to organize your mail, you might want to run the SpamSieve rule first. This will allow it to find spam among all your messages. If you would rather deal with spam manually than have any false positives, then you might want to run the SpamSieve rule last, after all your other rules have been given a chance to match and file away messages from known senders. Be sure to check the SpamSieve preferences for additional filtering options.

4.2 Apple Mail Rule Customization

4.2.1 Whitelisting Previous Recipients

For added safety, you can tell Mail that people who you've sent mail to will never send you spam. To do this, open the **Rules** section of Mail's **Preferences** window and edit the **SpamSieve** rule. Change the condition that says **Every Message** to **Sender is not in my Previous Recipients**. Mail will then assume that such messages are good, without showing them to SpamSieve. You might not want to do this, however, if you regularly receive spam messages that are *forged* so as to appear as though they were sent from one of your previous correspondents.

4.2.2 Automatically Deleting Old Spam Messages

Mail has a feature, accessible from the **Mailbox Behaviors** (or **Special Mailboxes**) tab of the **Accounts** preferences, that can automatically delete old spam messages from the **Junk** mailbox. You can use this feature if you tell SpamSieve to put spam messages in the **Junk** mailbox instead of the **Spam** mailbox.

(*Note:* If you do this, be careful not to use the **Junk** and **Not Junk** buttons that will appear in Mail when the **Junk** mailbox is active; you should always use the **SpamSieve - Train as Good** and **SpamSieve - Train as Spam** commands instead. You can use the **Customize Toolbar...** command in Mail's **View** menu to remove the **Junk** button from the toolbar. Also, if you select a message that SpamSieve has classified as spam, Mail will show a banner saying that *you* marked it as junk. Ignore this.)

To tell SpamSieve to use the **Junk** mailbox, open Mail's **Preferences** window and click on **Junk Mail**. Make sure that **Enable junk mail filtering** is checked. Select **Move it to the Junk mailbox**. If Mail asks whether you want to move all the messages to the Junk mailbox, say **No**. Select **Perform custom actions**. Then click the **Advanced...** button and edit the rule such that the conditions *don't match any messages*. For example, use these two conditions:

- Message *is* addressed to my Full Name

- Message *is not* addressed to my Full Name

Click **OK** to close the sheet. Do not make any further changes to the **Junk Mail** preferences. It should still be in **Automatic** mode, and you can ignore the rest of the window.

Go to the **Rules** section of Mail's preferences and change the SpamSieve rule to move the messages to the **Junk** mailbox instead of the **Spam** mailbox. Finally, choose **SpamSieve - Change Settings** from Mail's **Message** menu and, when prompted, say that the name of your spam mailbox is **Junk**.

4.2.3   Changing the Name of the Spam Mailbox

You can change the name of the mailbox where incoming spam messages are stored. For example, you might put a space in front of the name to make it sort to the top of your mailbox list. To do this, simply rename the **Spam** mailbox in Mail by selecting it and choosing **Rename**... from the **Mailbox** menu. The **SpamSieve** rule in Mail's preferences should automatically update to reflect the new mailbox name. (To change the spam mailbox to a different mailbox that already exists, open the **SpamSieve** rule in Mail's preferences and select that mailbox from the pop-up menu.)

Then choose **SpamSieve - Change Settings** from Mail's **Message** menu and, when prompted, enter the new mailbox name. This will tell SpamSieve where to put the messages when you use the **SpamSieve - Train as Spam** command. You can also enter the name of a different mailbox; some people like to enter **Deleted Messages** so that messages trained as spam are moved directly to the trash.

4.2.4   Marking Incoming Spam Messages

Normally, SpamSieve puts incoming spam messages in the **Spam** mailbox, and it colors them according to how spammy they are. You can customize this behavior by editing the actions of the **SpamSieve** rule in Mail's preferences. For example, to mark the spam messages as read, click the **+** button at the bottom of the rule sheet, and choose **Mark as Read** from the pop-up menu.

4.2.5   Redirecting Good Messages to Another Account

When traveling, especially if you have a Palm or BlackBerry, you might want to avoid downloading spam messages from the server. You can do this by letting your Mac at home filter the messages from your main mail account and redirect the non-spam messages to the account that you access when traveling. The spam messages will stay in the **Spam** mailbox on your Mac.

Open Mail's **Preferences** window and click the **Add Rule** button. Enter a description, such as "Redirect good messages to handheld." Change the condition from **From** to **Every message**. Then change the action from **Move Message** to **Redirect Message** and enter the e-mail address of the account that you check when traveling. Click **OK**. Finally, drag your newly created rule so that it is just below the **SpamSieve** rule.

4.2.6 Separate Spam Mailboxes for Each Account

Normally, SpamSieve puts the spam messages from all your Apple Mail accounts into a single mailbox called **Spam**. If you want to have a separate spam mailbox for each account, first create the requisite empty mailboxes. Then, create one rule in Mail for each account. The description for the rule should be **SpamSieve - [AccountName]** where **[AccountName]** is any text that helps you identify the account. The rule's condition should be that the account is **[AccountName]**, and the action should be to move the message to the spam mailbox for that account.

As this example demonstrates, you can have multiple SpamSieve rules in Apple Mail, with arbitrary conditions, so long as all of their descriptions start with **SpamSieve**. It is recommended that you arrange the conditions such that only one SpamSieve rule will be applied to any given message.

4.2.7 Setting up a Spam Filtering Drone

This tutorial from MacMerc[18] shows how to set up a spare Mac as a spam filtering drone. The idea is that multiple computers check the same IMAP account. One Mac (the drone) downloads all the messages and filters them with SpamSieve. The others (your main Mac, your PC at work, your iPhone, etc.) get a spam-free inbox. If a spam message gets through to your main Mac, you can drag it to the **AddToSpam** mailbox to train the drone. For any given IMAP account, there should be only only copy of SpamSieve (drone or regular) filtering its mail.

4.3 Entourage 2004 Rule Tips

A common situation is to have several Entourage rules that file incoming messages into different folders (perhaps based on the account or subject). If spam messages never match the criteria of these rules, then you can simply order these rules above the SpamSieve rule(s), so that SpamSieve only processes the messages that don't match your other rules.

If, however, you want SpamSieve to filter the messages *before* they are filed by the other rules, then you should follow the instructions in Two SpamSieve Rules and put the other rules below the SpamSieve rules.

---

[18]http://www.macmerc.com/articles/Mini_Media_Mac/368

4.4 Entourage v.X Rule Tips

Once an Entourage v.X rule runs an AppleScript or moves a message, it cannot apply any more rules to that message. This limitation means that extra steps are necessary to integrate SpamSieve into a complex set of Entourage rules. The easiest solution is to update to Entourage 2004 or 2008, which are more flexible about how they handle AppleScript rules. If you do not wish to do this, here are some possible workarounds:

- One option is to order your rules so that Entourage applies the SpamSieve rule after all your other rules. You can change the order of the rules by choosing **Rules** from Entourage's **Tools** menu and dragging the rules in the list to change their order. With this approach, you can filter your good messages into folders however you want. Any mail that is not moved into another folder will remain in your inbox. Then, the SpamSieve rule will either mark the spams as junk or move them to a **Junk E-mail** folder. The disadvantage to this approach is that SpamSieve cannot catch any spams among the messages that were moved by your other rules.

- Another option is to add the **Run AppleScript** action to each rule that moves messages. For instance, suppose you have a rule that moves all the messages from your **Work Account** account into a **Work** folder. You could set up the rule as shown below.

  Now, messages sent to that account will be moved to the **Work** folder. Spam messages sent to that account will be moved to the **Junk E-mail** folder. You can add the SpamSieve AppleScript action to every rule that moves messages and also to a "catch-all" rule that applies to messages that aren't moved. Then SpamSieve will be able to filter all the messages that you receive.
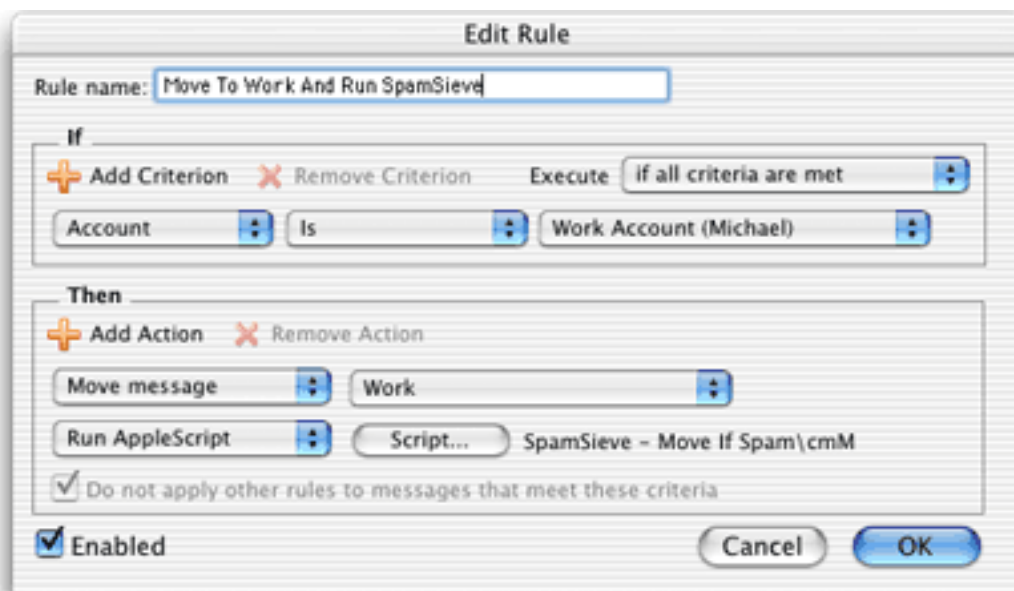
4.5 The Change Settings Command

Apple Mail and Entourage users can use the **SpamSieve - Change Settings** command to customize SpamSieve's behavior in those programs. In Apple Mail, this command is located in the **Message** menu; in Entourage, it is in the **Scripts** menu.

For Apple Mail, the settings are:

- Which mailbox should spam messages be moved to when you use "Train as Spam"?

- Should messages marked using "Train as Spam" be stored in a local spam mailbox (rather than on the server)? (This will use the spam mailbox for the first IMAP account that's listed in Mail's preferences.)

- Should "Train as Spam" mark the messages as read?

- When you use "Train as Good" on a message in the spam mailbox, should the message be moved back to the inbox?

- When you use "Train as Good" on a message in the spam mailbox, should the message be marked as unread¿'

- Should incoming spam messages be colored according to how spammy they are (darker means more spammy)?

For Entourage, the settings are:

- Which folder should spam messages be moved to when you use "Train Spam"?

- Should "Train Spam" mark the messages as read?

- When you use "Train Good" on a message in the spam folder, should the message be moved back to the inbox?

- When you use "Train Good" on a message in the spam folder, should the message be marked as unread?

- Which folder should incoming spam messages be moved to? (This only affects POP messages. For IMAP and Exchange messages, you would need to modify the **SpamSieve - Move Messages** rule.)

- Should incoming spam messages be marked as read?

- Should incoming spam messages be removed from the mail server?

- Should incoming spam messages be marked with category "Uncertain Junk" rather than "Junk" if SpamSieve thinks they are not as spammy?

For other mail programs, similar options are available either in the mail program's preferences, or by editing the SpamSieve rule.

4.6 Additional AppleScripts

Many aspects of SpamSieve are scriptable, and it is possible to customize SpamSieve and extend its features using AppleScript. A collection of commonly requested example scripts[19] is available.

4.7 Integrating With Other Applications

SpamSieve's interface for integrating with third-party mail and news programs is completely open. It is possible to add support for additional programs simply by writing some AppleScripts or Apple event code. SpamSieve's AppleScript dictionary contains some basic information about the supported commands. However, there are some subtle, but important, points that are not discussed in the dictionary's documentation. If you would like to connect an application to SpamSieve, please contact spamsieve@c-command.com[20] so that I may assist you.

5 Menus

5.1 The SpamSieve Menu

5.1.1 About SpamSieve

The **About SpamSieve** window shows the credits, download and support information, and the current version numbers of SpamSieve's plug-ins.

You can always download the latest version of SpamSieve from the SpamSieve Web site[21].

Questions about SpamSieve may be sent to spamsieve@c-command.com[22]. I'm always looking to improve SpamSieve, so please feel free to send any feature requests to that address.

To make sure that you have the latest version of SpamSieve, you can use the Software Update feature or subscribe to the SpamSieve News mailing list[23]. The traffic on this list is very low, only one message per new version of SpamSieve.

The SpamSieve RSS feed[24] contains update notices and other SpamSieve news.

The SpamSieve forum[25] is the place to talk with other SpamSieve users, share tips and tricks, and

---

[19]http://c-command.com/scripts/spamsieve/
[20]mailto:spamsieve@c-command.com
[21]http://c-command.com/spamsieve/
[22]mailto:spamsieve@c-command.com
[23]http://c-command.com/spamsieve/support
[24]http://c-command.com/blog/category/spamsieve/feed
[25]http://c-command.com/forums/forumdisplay.php?f=1

ask questions.

5.1.2 Software Update

Click the **Check Now** button, and SpamSieve will tell you whether a newer version is available for download. By default, SpamSieve will automatically check for new versions each time it is launched and once per day. You can disable this feature by unchecking the checkbox.

If a new version is available, SpamSieve will tell you what's new in that version. Click **Download** to have SpamSieve download the `.dmg` file for the new version to your Internet downloads folder. Click **Download & Install** to have it download the `.dmg` and then update the installed SpamSieve application to the new version.

To check for a new version, SpamSieve contacts a Web server at `dreamhost.com`. SpamSieve transmits the following information to the server: the name of the product (SpamSieve) and its version, the version of Mac OS X, whether SpamSieve is registered, the name of the current mail program, and the name of the current language. This information is used to guide future development. No personal information is transmitted.

5.1.3 Purchase

This window lets you buy SpamSieve. If you've already purchased SpamSieve but it's running in demo mode, you can you enter your name and serial number to personalize your copy of SpamSieve and remove the demo limitations.

SpamSieve has a free trial period that lasts for 30 days or 7 launches, whichever is longer. To use SpamSieve beyond the demo period, you must purchase it. This entitles you to free updates and support.

To purchase, choose **Purchase...** from the **SpamSieve** menu. You can use the **Purchase** button to enter the online store.

Soon after paying, you'll receive an e-mail with your serial number. Enter the name and serial number from the e-mail into the **Purchase** window and click **Personalize**. If you need to re-install SpamSieve, you can simply re-enter your name and serial number and click **Personalize**; there's no need to purchase again.

If you purchased SpamSieve but cannot find your serial number, click the **Lost Your Serial Number?** button. This will open a form where you can enter your e-mail address and look up your order information.

A license for SpamSieve is good for one person *or* one computer. You can install it on one Mac, and everyone sharing that Mac can use it (on that Mac). Alternatively, you can install it on your

desktop Mac and your laptop; you can then use it on either machine, provided that no one is using it on the other machine.

5.1.4   Install Apple Mail Plug-In

This command installs (or updates) the plug-in that SpamSieve uses to integrate with Apple Mail.

5.1.5   Install Entourage Scripts

This command installs (or updates) the AppleScript files that SpamSieve uses to integrate with Entourage. Occasionally, the script files can become damaged, causing Entourage to ask you to locate the SpamSieve application each time you receive mail or try to train SpamSieve. Using this command to install fresh copies of the scripts (and letting it replace the old ones, when it asks you) should fix that problem.

5.1.6   Install Eudora Plug-In

This command installs (or updates) the plug-in that Eudora 6 uses to communicate with SpamSieve. It also disables any other Eudora junk mail plug-ins, as they would conflict with SpamSieve. The SpamSieve Eudora plug-in is installed in the folder:

```
/Users/<username>/Library/Application Support/Eudora/PlugIns/
```

5.1.7   Show Other Scripts

This opens a folder containing AppleScript files for integrating SpamSieve with DragThing, Emailer, Eudora 5.2, Outlook Express, PowerMail 4, and Mailsmith. These can be installed by dragging them into the proper locations.

Opening the containing folder (using Command-Up-Arrow) reveals the scripts for Entourage, as well as SpamSieve's plug-ins for Apple Mail and Eudora 6. Normally, there is no need to access these items directly, as SpamSieve can install them automatically (see above). They are accessible here in case you want to install them manually.

5.1.8   Update Address Book "Me" Card

When you use this command, SpamSieve looks at the account information for any e-mail programs that are currently running and adds any e-mail addresses that it finds to the "Me" card of the

system address book. SpamSieve uses the addresses on this card to determine when a message that you receive includes your return address. This can help it detect spam messages that were forged to look like you sent them, in conjunction with the Exclude my addresses preference. Also, SpamSieve will avoid automatically creating whitelist rules for addresses listed on the "Me" card.

5.2   The File Menu

5.2.1   Import Addresses...

This imports either good or spam e-mail addresses from a text file. For each address, a rule is created on the whitelist (or blocklist) that matches messages sent from that address. If such a rule already exists, SpamSieve makes sure that it's enabled. Rules in the opposite list are not affected.

Many file formats are supported: the addresses can be return- or comma-delimited, or they can be mixed in with message text as part of a mbox file.

- To import addresses from Entourage, choose **Export**... from the **File** menu and select the option to **Export contacts to a tab-delimited text file**.

- To import addresses from Eudora, ask SpamSieve to import the `Eudora Nicknames` file inside the `Eudora Folder` (which is likely in your `Documents` folder).

- To import addresses from the Mac OS X address book, open the Address Book program. Choose **Card and Columns** from the **View** menu. Select all the names in the middle column (**Name**) and drag them to the desktop. This will create a `.vcf` file, which you can import into SpamSieve.

You may be wondering why you would want to import addresses from the Mac OS X address book instead of using the Use Mac OS X Address Book preference, or why you would import addresses from Entourage instead of using the Use Entourage address book preference. The difference is as follows. When you ask SpamSieve to use an address book directly, it will *always* consider messages from senders in the address book to be good—even if you receive many spam messages that are forged to appear as if they were sent by your friends.

When the addresses are imported to the whitelist, however, they are subject to SpamSieve's normal whitelist behavior. That is, if Train SpamSieve whitelist is checked, when you receive a spam message from someone on the whitelist, SpamSieve will *disable* the corresponding whitelist rule. Subsequent messages from that sender will no longer be whitelisted. In short, the address book is safer because it makes sure messages from people in your address book *always* get through. The whitelist is less safe, but it allows you to block forged spam messages.

If you prefer the address book behavior but don't have all of your addresses entered into the address book, you can use **Import Addresses**... to create whitelist rules from your addresses, and then

select the rules and use this script[26] to convert the rules into address book cards.

Imported address files must be less than 400K; to import more addresses, break the file into smaller chunks.

5.2.2   Import Corpus...

This imports the words in a corpus that was exported in XML format. This is the same format used by SpamSieve 1.x. Importing a corpus *merges* it with the active corpus. To *replace* the active corpus with the one you are importing, use the **Reset Corpus**... command before importing.

5.2.3   Export Corpus...

This exports the active corpus to XML format. You might do this in order to import the corpus on another machine.

5.3   The Filter Menu

5.3.1   Show Corpus

The corpus is a collection of messages, both spam and good, with which you have trained SpamSieve. SpamSieve's Bayesian classifier analyzes the contents of the messages and uses this information to predict whether future messages are spam or good. The contents of the corpus are managed by SpamSieve; therefore, once you've trained SpamSieve with a message, deleting the message from your e-mail program will not affect SpamSieve because the information from that message is stored in the corpus.

---

[26]http://c-command.com/scripts/spamsieve/whitelist-to-address-book

Word	Spam	Good	Total	Prob. ▲	Last Used
readiness	6	0	6	0.999	7/25/06
RP:@createacd.com	6	0	6	0.999	6/5/06
S:cheaper	6	0	6	0.999	7/27/06
S:earn?	6	0	6	0.999	7/27/06
S:pleasure	6	0	6	0.999	7/23/06
seaweed	6	0	6	0.999	7/25/06
sportswear	6	0	6	0.999	7/25/06
beams	7	0	7	0.999	7/25/06
beatrice	7	0	7	0.999	7/25/06
breakout	7	0	7	0.999	7/27/06
dearest	7	0	7	0.999	7/27/06
jealousy	7	0	7	0.999	7/27/06
peach	7	0	7	0.999	7/27/06
R:^pitt^east^verizon^net	7	0	7	0.999	7/27/06
RP:@reach.net.th	7	0	7	0.999	6/23/06
RT:leanie	7	0	7	0.999	7/11/06

The **Show Corpus** command opens the **Corpus** window so that you can examine the words that SpamSieve has found in your e-mails. You can click on the name of a column to sort by that column. Click again on the column to reverse the sort direction. The meanings of the columns are as follows:

Word

A word in the corpus.

Spam

The number of times the word has occurred in spam messages.

Good

The number of times the word has occurred in good messages.

Total

The total number of times the word has occurred.

Prob.

> The probability that a message is spam, given that it contains the word (and in the absence of other evidence).

Last Used

> The date that the word was added to the corpus, or the date that it last appeared in a received message (whichever is later).

You can copy the selected rows to the clipboard or drag and drop them into another application.

With the window sorted by **Word**, you can type the first few letters of a word to locate that word in the corpus. Similarly, you can sort by one of the other columns and type a number to locate the first word whose value for the sorted column matches the number you typed.

You can edit the spam and good counts associated with a word by double-clicking on the number in the **Spam** or **Good** column. Changing the numbers for important words can greatly affect SpamSieve's accuracy, so you shouldn't make changes without good reason.

You can remove words that you don't want in the corpus by selecting them and pressing Delete.

5.3.2   Reset Corpus...

This command removes all the words and messages from the corpus. (It does not change the whitelist or blocklist.) After resetting the corpus, you can retrain SpamSieve from scratch, and SpamSieve will let you use your old messages in the retraining. Resetting the corpus and re-training SpamSieve with a proper mix of recent messages can increase SpamSieve's accuracy and reduce its memory use.

Before you reset the corpus, SpamSieve automatically saves a backup in case you need to go back to the old corpus. The backups are saved in this folder:

```
/Users/<username>/Library/Application Support/SpamSieve/
```

To restore from a backup, choose **Import Corpus**... from the **File** menu and choose the appropriate `Corpus <date>.plist` file.

5.3.3   Show Statistics

This command opens the **Statistics** window, which displays the following information:

Good Messages

> The number of non-spam messages that SpamSieve has filtered.

Spam Messages

The number of spam messages that SpamSieve has filtered.

Spam Messages Per Day

The average number of spam messages received per 24-hour period.

False Positives

The number of good messages that SpamSieve identified as spam.

False Negatives

The number of spam messages that SpamSieve identified as good.

% Correct

The percent of messages that SpamSieve identified correctly.

Good Messages

The number of non-spam messages that are used to identify spam messages.

Spam Messages

The number of spam messages that are used to identify spam messages.

Total Words

The total number of unique words in the corpus.

Blocklist Rules

The number of rules on SpamSieve's blocklist.

Whitelist Rules

The number of rules on SpamSieve's whitelist.

Statistics

Filtered Mail

1,823 Good Messages

31,538 Spam Messages (95%)

3,290 Spam Messages Per Day

SpamSieve Accuracy

0 False Positives

34 False Negatives

99.9% Correct

Corpus

3,692 Good Messages

7,095 Spam Messages (66%)

134,530 Total Words

Rules

8,181 Blocklist Rules

17,489 Whitelist Rules

Showing Statistics Since

5/5/08 1:00 AM

Set Date...   Copy Stats

You can copy all the statistics to the clipboard using the **Copy** command in the **Edit** menu or by clicking the **Copy Stats** button.

Normally, SpamSieve shows statistics for all the messages that it processed since it was installed. Because the accuracy and the number of messages you receive change with time, you may wish to only see recent statistics. Click the **Set Date...** button at the bottom of the window to control which old statistics are hidden from view. You can edit the date and time shown in the sheet, or enter an entirely new date. SpamSieve will accept dates specified in natural language, such as "last

Sunday at dinner" or "today." The **Now** button enters the current date and time.

5.3.4 Open Log

SpamSieve keeps a log of messages that it has filtered, words that it has used to decide whether the messages were spam, messages you have added to the corpus, and any errors that have occurred. This command opens the log file so that you can look at it. Normally, there is no reason (aside from curiosity) to look at the log file. However, if you believe SpamSieve is not working as it should, the log file provides useful information about what SpamSieve has done.

1. For each incoming message, there should be an entry in SpamSieve's log that says `Predicted:  Good` or `Predicted:  Spam`. If you see only `Trained:` entries (or no entries at all) for a message, then the mail program did not ask SpamSieve to analyze that message, and you should check the setup.

2. If SpamSieve left a spam message in your inbox, there will be a `Predicted:  Good` entry for that message in the log. The `Reason` can provide clues for why SpamSieve thought the message was good.

   - If it says `sender <address> in address book`, you might want to remove that address from address book, add it to the Me card, or else uncheck SpamSieve's option to Use Mac OS X Address Book.
   - If it says `sender <address> in Entourage address book`, you might want to remove that address from Entourage's address book (then click **Load** while holding down the Option key) or uncheck SpamSieve's option to Use Entourage address book.
   - If spam messages are being predicted as good and you don't understand why, please send in a report.

3. If SpamSieve moved a good message to the spam folder, there will be a `Predicted:  Spam` entry for that message in the log. The `Reason` can provide clues for why SpamSieve thought the message was spam.

If you find that the log file is taking up too much disk space, you can delete it at any time. SpamSieve will then start a new log file as needed.

5.3.5 Edit Log
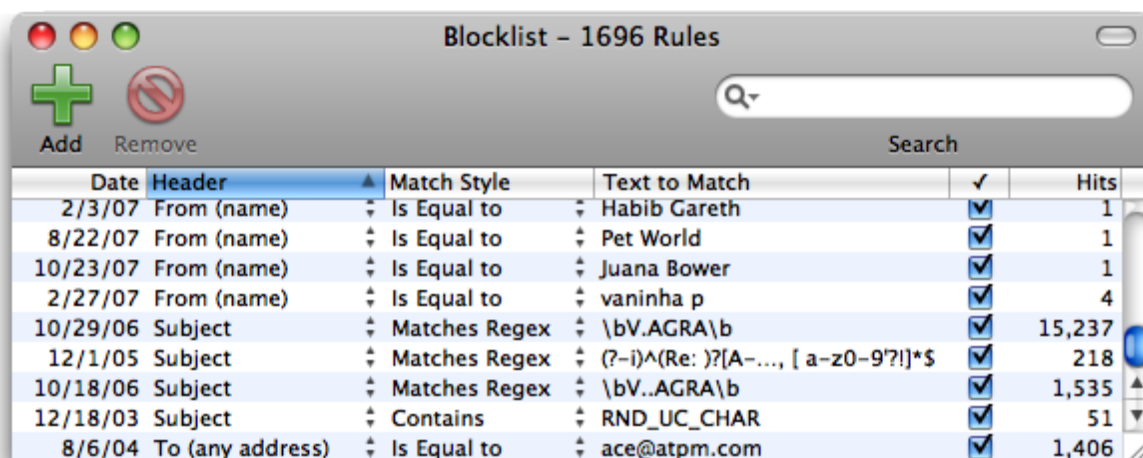
This command opens the log file in a text editor such as TextEdit or TextWrangler[27] instead of Console. This makes it easier to read and search large log files.

---

[27]http://www.barebones.com/products/textwrangler/index.shtml

5.3.6   Show Blocklist

This opens the **Blocklist** window. The blocklist consists of a list of *rules*. If a message *matches* one or more rules on the blocklist, SpamSieve will predict that it is spam. Each row in the blocklist window represents one rule.

The meanings of the columns are as follows:

Date

  The date that the rule was added to the blocklist.

Header

  The part of the message that will be matched against the rule.

Match Style

  How the rule text will be matched against the text from the message's header.

Text to match

  The text that will be matched against the message's header.

√

  If this is checked, the rule is enabled. Disabled rules do not block any messages, but they are useful because they prevent SpamSieve from re-learning a rule that you don't want.

  For example, say that you get forged spam messages from your own address. When you receive such a message, and tell SpamSieve that it's spam, any rule on the whitelist with your address would be disabled. This will enable future such messages to be caught. If you later get a legitimate message from your own address and tell SpamSieve that it's good, the whitelist rule will remain disabled. If you had previously deleted the rule instead of disabling

it, telling SpamSieve that the message was good would create a new, enabled whitelist rule, which is probably not what you want.

Hits

The number of spam messages that the rule blocked, a rough measure of how effective it is.

When SpamSieve checks whether a message matches a rule, it compares the part of the message named by the **Header** column with the contents of the rule's **Text to Match** column. The following are the message parts that may be used in the **Header** column:

From (address)

The e-mail address of the message's sender.

From (name)

The name of the message's sender.

To (any address)

The e-mail addresses of the primary recipients of the message. SpamSieve checks each recipient separately to see whether it matches the rule.

CC (any address)

The e-mail addresses of the carbon copy recipients of the message. SpamSieve checks each recipient separately to see whether it matches the rule.

Reply-To (address)

The address that you would be sending to if you replied to the message. This is often the same as the From address, but it could also be a mailing list or an alternate address for the sender. If the message does not specify a Reply-To, then the rule will not match.

Any Recipient

The To and CC addresses.

Any Address

The From, To, CC, Reply-To, and SendTo addresses.

List-ID

For mailing list messages, this hidden header indicates which mailing list the message was sent to.

List-Unsubscribe

For mailing list messages, this hidden header indicates how to unsubscribe from the mailing list. Some mailing list messages that do not have a List-ID header do have a List-Unsubscribe header.

Mailing-List

For mailing list messages, this hidden header indicates which mailing list the message was sent to. Some mailing list messages that do not have a List-ID header do have a Mailing-List header.

Received (any)

The Received headers contain information about the servers that relayed the message on its journey from the sender to the recipient.

Return-Path

This header contains information about where the message originated.

Subject

The subject of the message.

Body (any text part)

The contents of the message. Some messages contain more than one text part (for instance, plain text and HTML representations of the same message). The rule matches the message if any of the text parts matches the rule's text.

Any Character Set

The character set often indicates the language of the message. Many spam messages are sent using Asian or Cyrillic character sets, and SpamSieve is pre-configured to block these. The IANA maintains a list of character sets[28].

Any Attachment Name

Many spam messages contain attachments whose names end with `.pif` or `.scr`. SpamSieve ships with some blocklist rules pre-configured to catch messages containing spammy attachments.

There are several different ways in which SpamSieve can compare the text in the message's header to the rule's text. In all cases, capitalization does not matter; lowercase letters are considered the same as their uppercase counterparts.

Is Equal to

The message matches the rule if its text is exactly the same as the rule's text. This is the fastest style of matching. If you leave the text blank, the rule will match messages that have *blank* values for that header—for example when there is an empty Subject header. Sometimes, messages (especially spam ones) *omit* headers. To match an omitted header, enter `<SpamSieve-Unknown-Subject>`, `<SpamSieve-Unknown-From>`, `<SpamSieve-Unknown-FromName>`, or `<SpamSieve-Unknown-To>` depending on the header selected.

---

[28]`http://www.iana.org/assignments/character-sets`

Contains

The message matches the rule if the message text contains the rule text.

Starts with

The message matches the rule if the message text begins with the rule text.

Ends with

The message matches the rule if the message text ends with the rule text. This is useful for matching domain names. For example, to match messages sent from Apple, you could create an **Ends with** rule with text `@apple.com`.

Matches Regex

This is like Contains, except that the rule text is treated as a Perl-compatible[29] regular expression[30]. Regular expressions are a powerful way of specifying patterns of text, for instance: e-mail addresses that contain numbers before the @ sign or subjects that are longer than 30 characters. For example, a **Matches Regex** rule with the text:

`^.*(?<!^sales|^support)@domain\.com$`

would match all messages where the match field ends with `@domain.com` but is not `sales@domain.com` or `support@domain.com`. This can be used to block messages sent to fake addresses[31]. And this regex:

`(?-i)^(Re: )?[A-Z]{2,8}, [ a-z0-9'?!]*$`

matches a common pattern of spam message subjects.

If the regular expression entered in the **Text to Match** column is invalid, SpamSieve will color it in red, and it will not match any messages.

You can edit a rule's **Header** or **Match Style** by clicking in the corresponding column and selecting from the pop-up menu. To edit a rule's **Text to Match**, double-click the text.

Training SpamSieve with a spam message adds its sender to the blocklist. You can delete a rule from the blocklist by selecting it and pressing Delete. Generally, there is little reason to delete rules; if you don't like what a rule is doing, you should instead uncheck the rule to prevent SpamSieve from re-learning it. Also, SpamSieve is optimized such that having lots of rules does not reduce performance.

You can copy the selected rules to the clipboard or drag and drop them into another application. You can type the first few letters of a rule's **Text to Match** to quickly locate that rule, or use the search field in the toolbar to focus on a group of related rules.

---
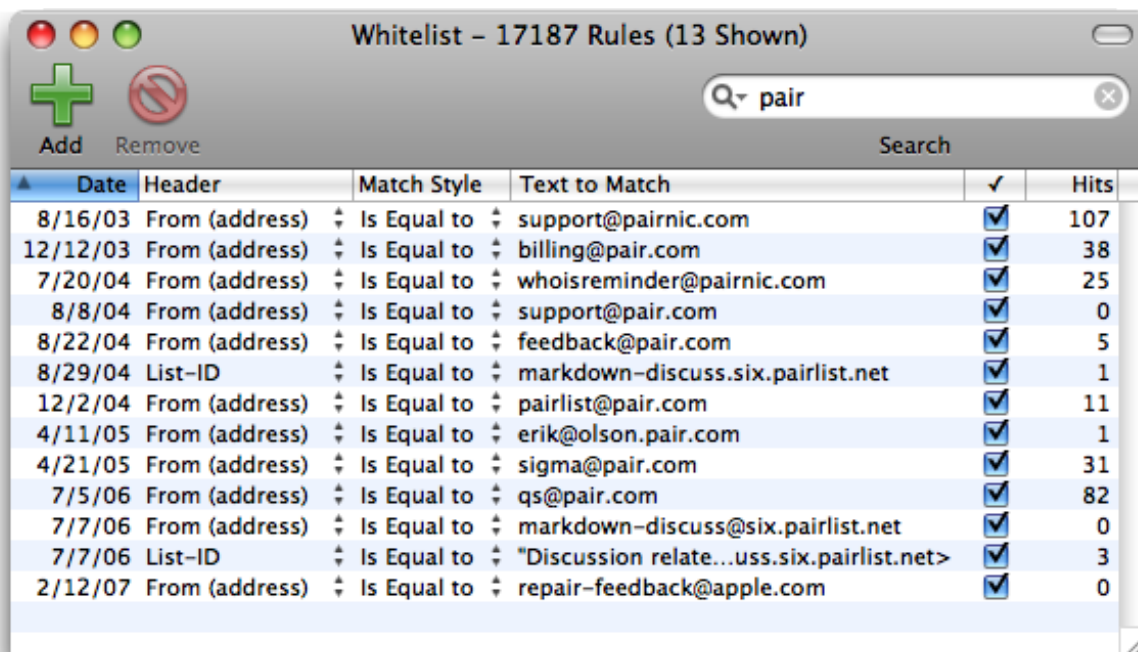
[29]`http://pcre.org/pcre.txt`
[30]`http://en.wikipedia.org/wiki/Regular_expressions`
[31]`http://c-command.com/blog/2006/06/22/fake-addresses/`

5.3.7 Show Whitelist

The whitelist works the same way as the blocklist except that messages sent from addresses on the whitelist are *never* considered to be spam. The whitelist also has special support for mailing lists. If you train SpamSieve with a good message from a mailing list, it will add a rule to the whitelist that matches the message's mailing list header (List-ID, List-Unsubscribe, or Mailing-List). Then SpamSieve will know that all messages from that mailing list are good, regardless of who sent them.

The whitelist is most commonly used for matching messages sent from particular addresses, domains, or mailing lists. You can also use the whitelist to create *codewords*. For instance, you could create a rule in the whitelist that matches subjects containing "eggplant" (or some other word unlikely to occur in regular mail). You can tell select people to put "eggplant" in the subject of messages that they send you, and then you can be assured that their messages will get through, *even if the sender addresses are not in your address book or whitelist.*

5.3.8 Add Rule

This command creates a new rule in either the whitelist or blocklist. This is useful if you want to add your own rules to the whitelist or blocklist, rather than having SpamSieve learn the rules when you train it with messages. For example, you could create a blocklist rule to catch spam messages with a particular subject, or a whitelist rule to always accept messages sent from a certain domain.

5.3.9 Show Training Tip

This opens the **Training Tip** window, which gives advice for improving SpamSieve's accuracy, based on your current corpus.

6 Preferences

6.1 Filters

SpamSieve uses a variety of filters to determine whether messages are spam or good. It consults the filters in the order listed in this window. When a filter decides that the message is good or spam, SpamSieve stops moving down the list. Thus, the order of the filters makes a difference. You can see from the order that if a message's sender is on the whitelist, it will be marked as good even if the Bayesian classifier would have predicted it to be spam. Normally this is what you want; the point of a whitelist is that you can be sure that certain messages will *never* be marked as spam.
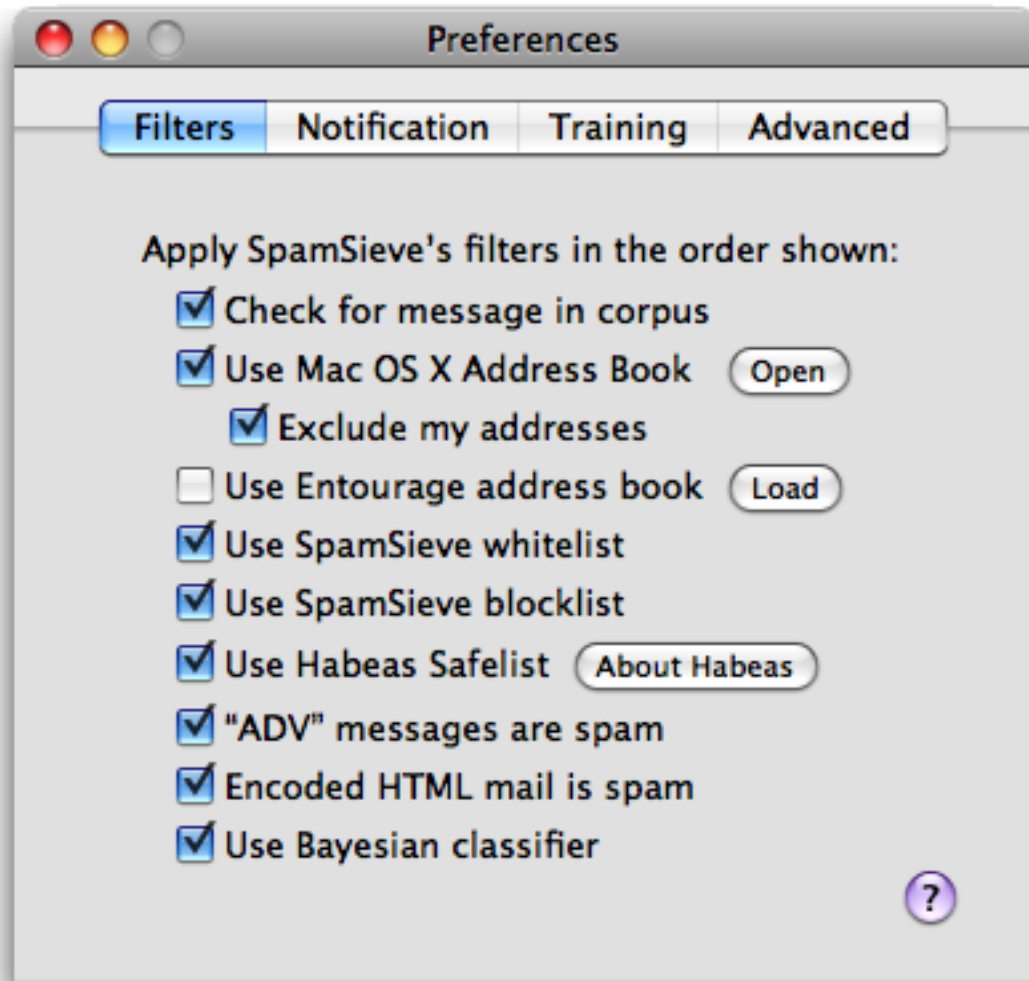
6.1.1 Check for message in corpus

SpamSieve learns as you train it, but training is not instant. Training SpamSieve with a message will not necessarily give it enough information to classify that message correctly based only on the words in the message. However, once you have added a message to the corpus, SpamSieve *knows* whether it is good or spam, even though it might not make the correct prediction based on word probabilities. This option causes SpamSieve to see if it knows whether a message is good or spam before trying to calculate its spam probability. If SpamSieve has seen the message before, it will always classify it correctly. You can disable this option if you want to see what SpamSieve would have predicted if it did not already know whether the message was good or spam.

6.1.2   Use Mac OS X Address Book

With this option enabled, SpamSieve will never predict a message to be spam if its sender's e-mail address is in the system address book.

You can add addresses to the system address book using the Address Book application (located in the `/Applications` folder), or directly from an e-mail program that supports the system address book.

Mailsmith and PowerMail users should be sure to enable the option to use Apple's Address Book. Entourage users may prefer to use their address book as a whitelist instead of Apple's. This is described in the Entourage section.

If spam messages get through to your inbox because they are sent from addresses in your address book, you can either uncheck **Use Mac OS X Address Book** or see Exclude my addresses.

6.1.3   Exclude my addresses

Enable this option so that spam messages with your own return address are not marked as good. (Spammers sometimes forge the return address to be your own, in an attempt to get through spam filters.) Disable this option if you send yourself messages and want to make sure that they are never marked as spam. SpamSieve looks on the "Me" card in Apple's Address Book to determine which addresses are yours. The easiest way to add your addresses to the "Me" card is to open your mail program and then use SpamSieve's Update Address Book "Me" Card command.

You can also use this feature to catch spam messages sent from certain addresses in your address book. Normally, if you have Use Mac OS X Address Book checked, messages from addresses in your address book will never be classified as spam. This is generally what you want, but there may be one or two particular addresses that spammers keep forging. By using **Exclude my addresses** and adding those addresses to the "Me" card in Address Book, you can get SpamSieve to analyze the full contents of those messages to determine whether they are spam. SpamSieve will continue to use the other addresses in the address book as before, always classifying messages from them as good.

6.1.4   Use Entourage address book

This option and the **Load** button are not needed if you have Entourage 11.2.3 or later and have **Synchronize contacts with Address Book and .Mac** checked in Entourage's preferences.

With this option enabled, SpamSieve will not predict a message to be spam if its sender's e-mail address is in the Entourage address book. However, if you have **Exclude my addresses** checked, addresses on the Mac OS X address book's "Me" card will not be checked against Entourage's address book. This helps prevent forged spams from getting through.

When you start using SpamSieve, you should click the **Load** button to make SpamSieve read in the addresses in the Entourage address book. (This will cause SpamSieve to launch Entourage if it is not already open.) The addresses are loaded into SpamSieve's memory and stored in its preferences file, but they are not displayed in the **Whitelist** window because they are not whitelist rules.

If you have multiple Entourage identities, you can load the addresses into SpamSieve in sequence. Click **Load**, then change to another identity and click **Load** again, etc.

Whenever you *add* addresses to the Entourage address book, you should go back to SpamSieve's preferences and click **Load** so that SpamSieve learns about the new addresses. If you *remove* addresses from the Entourage address book, you should hold down the Option key when clicking **Load**; this tells SpamSieve to forget the old addresses before loading the new ones. Do not click **Load** while Entourage is downloading and filtering mail, as this may cause it to freeze.

Note that the **Load** button will not work unless **Warn before allowing an external application to access the address book** is unchecked in Entourage's **Security** preferences.

6.1.5   Use SpamSieve whitelist

Enable this option so that messages that match (enabled) rules on the SpamSieve whitelist are never marked as spam.

6.1.6   Use SpamSieve blocklist

Enable this option so that messages that match (enabled) rules on the SpamSieve blocklist are always marked as spam.

6.1.7   Use Habeas Safelist

The Habeas Safelist[32] is list of senders who agree to only send e-mail that meets Habeas' stringent compliance requirements. With this option checked, SpamSieve will consider a message to be non-spam if finds the sending mail server's IP address on the Habeas Safelist. This entails contacting Habeas' server to lookup the address, but there is little performance penalty for doing this, since SpamSieve only contacts the server when the message contains Habeas headers:

```
X-Habeas-SWE-1: winter into spring
X-Habeas-SWE-2: brightly anticipated
X-Habeas-SWE-3: like Habeas SWE (tm)
X-Habeas-SWE-4: Copyright 2002 Habeas (tm)
X-Habeas-SWE-5: Sender Warranted Email (SWE) (tm). The sender of this
```

---

[32]http://c-command.com/aboutHabeas

```
X-Habeas-SWE-6: email in exchange for a license for this Habeas
X-Habeas-SWE-7: warrant mark warrants that this is a Habeas Compliant
X-Habeas-SWE-8: Message (HCM) and not spam. Please report use of this
X-Habeas-SWE-9: mark in spam to <http://www.habeas.com/report/>.
```

or:

```
Accreditor: Habeas
X-Habeas-Report: Please report use of this mark in spam to <http://www.habeas.com/report/>
```

6.1.8 "ADV" messages are spam

This option causes SpamSieve to always mark messages as spam if they contain some variant of "ADV" at the start of the subject line. The "ADV" marker is used by some commercial bulk mailers.

6.1.9 Encoded HTML mail is spam

Many spammers *encode* the contents of their messages with base-64 so that filters cannot see the incriminating words they contain. SpamSieve can decode and look inside these messages. This option causes it to mark *all* such as spam, regardless of their contents, on the theory that legitimate senders do not try to obscure their messages. This does *not* affect messages *encrypted* with PGP[33].

6.1.10 Use Bayesian classifier

This enables SpamSieve's main spam detector, which uses the corpus and word probabilities to identify spam messages.

6.2 Notification

All e-mail programs can notify you when you receive new messages, but some will also notify you *even* when all the new messages are spam. If your e-mail program is not savvy in this way, you can turn off its notification and let SpamSieve notify you only when there are new good messages.

---

[33]http://www.pgp.com/products/desktop/personal/index.html
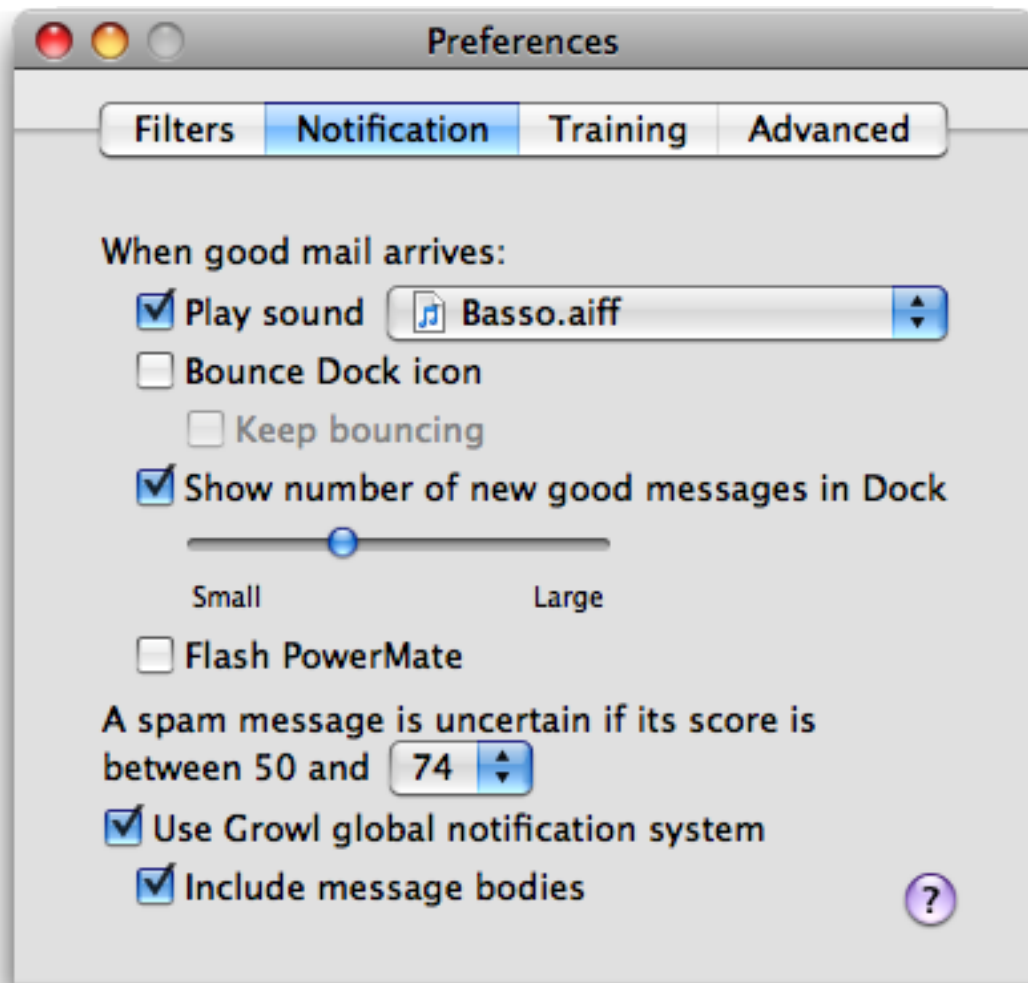
6.2.1 Play sound

This makes SpamSieve play a sound when new good messages are received. To add a sound to the menu, copy the sound file to the `Sounds` folder in your `Library` folder. SpamSieve will also look for sounds that are built into your installed e-mail programs.

6.2.2 Bounce Dock icon

This makes SpamSieve bounce its Dock icon once when new good messages are received.

6.2.3 Keep bouncing

You might not be looking at the Dock icon when it first bounces, so this makes SpamSieve continue bouncing its Dock icon until you activate SpamSieve or your e-mail program.

6.2.4 Show number of new good messages in Dock

This option makes SpamSieve show the number of new good messages in its Dock icon. If there are no new good messages or if SpamSieve or the mail program is frontmost, SpamSieve will not show any number (rather than showing zero). Clicking the Dock icon, activating your e-mail program, or training SpamSieve with a message will reset the count.

The slider lets you control the size of the number in the Dock icon.

If you're using DragThing[34] 5.3 or later, SpamSieve can show the message count in its tile in DragThing's process dock. With DragThing 5.3 and 5.3.1, you will need to install a file to enable this integration. Choose **Show Other Scripts** from the **SpamSieve** menu, and then open the `For DragThing Users` folder. In a separate window, locate the DragThing application. Control-click on the DragThing icon and choose **Show Package Contents**. Open the `Contents` folder and then the `Resources` folder. Control-click on the `DragThing Helper` file and choose **Show Package Contents**. Open the `Contents` folder and then the `Resources` folder. Drag the `mtSS.scpt` file from the `For DragThing Users` window into the `Scripts` folder in the `Resources` window.

6.2.5 Flash PowerMate

If you have a Griffin PowerMate[35], this option will make it flash when new good messages arrive. The flashing will stop when you activate SpamSieve or your mail program.

To change the rate of the pulsing, open System Preferences and go to the PowerMate pane. Adjust the **Rate** slider in the **Pulsing** section of the window.

This feature is compatible with versions 1.6.4 and 2.1 of the PowerMate software.

6.2.6 A spam message is uncertain if

SpamSieve assigns each message a score between 0 and 100, and it considers messages with scores 50 or greater to be spam. Message with scores above 90 are almost certainly spam. Most messages with scores in the 70s are also spam, but if there are any false positives they will likely be in this range.

---

[34]http://www.dragthing.com
[35]http://www.griffintechnology.com/products/powermate/

The pop-up menu lets you control the range of scores that SpamSieve considers to be *uncertain*. Uncertain messages may be assigned a different Entourage category, or they may be announced by an Uncertain Spam notification. In addition, messages in Apple Mail are colored according to their scores; uncertain messages will have backgrounds with brighter colors. By making it easier to spot uncertain messages, these mechanisms help you to efficiently verify whether SpamSieve has filtered your mail correctly.

Uncertain messages are considered to be spam, unless you tell SpamSieve otherwise; if you have auto-training on, there is no need to train SpamSieve that they are spam.

6.2.7   Use Growl global notification system

Growl[36] is a free, third-party package that can enhance SpamSieve's notification abilities. Once you have downloaded and installed Growl, the next time SpamSieve is launched it will use Growl to notify you when new messages arrive. You can customize the notification style and enable/disable notifications using the Growl pane in System Preferences.
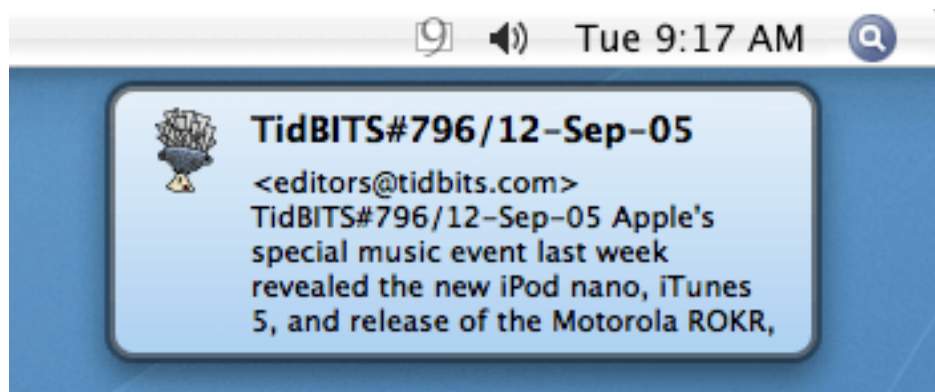
The following notifications are available:

Good Message Count

> This notification mimics the red number in SpamSieve's Dock icon. After a batch of good messages arrives, it tells you how many new messages there are and then fades away.

Good Messages (in Address Book)

> This posts one notification for each good message that arrives (where the sender is in your address book), showing the message's subject, the first few lines of its body, and (if possible) a picture of the sender.

---

[36]http://www.growl.info

Good Messages (Not in Address Book)

> This posts one notification for each good message that arrives (where the sender is *not* in your address book), showing the message's subject and the first few lines of its body.

Uncertain Spam

> This notification helps you spot false positives by telling you when a message has arrived that SpamSieve thinks is spam, but that may actually be good. In SpamSieve's preferences, you can set the score range for "uncertain spam", and then you will get a Growl notification for each message with a score in this range. By watching these notifications, you can spot false positives without having to look through the entire contents of the spam folder in your mail program. Unlike the other notifications, Uncertain Spam notifications will persist until you click to dismiss them.

If you are not using Growl, turn off this option in order to improve performance.

6.2.8   Include message bodies

Growl notifications always include the message's subject and sender. This setting controls whether they also include the first few lines of the message's body. Including the message body provides more context, which is particularly useful for Uncertain Spam notifications, but it also uses more screen space.

6.3   Training
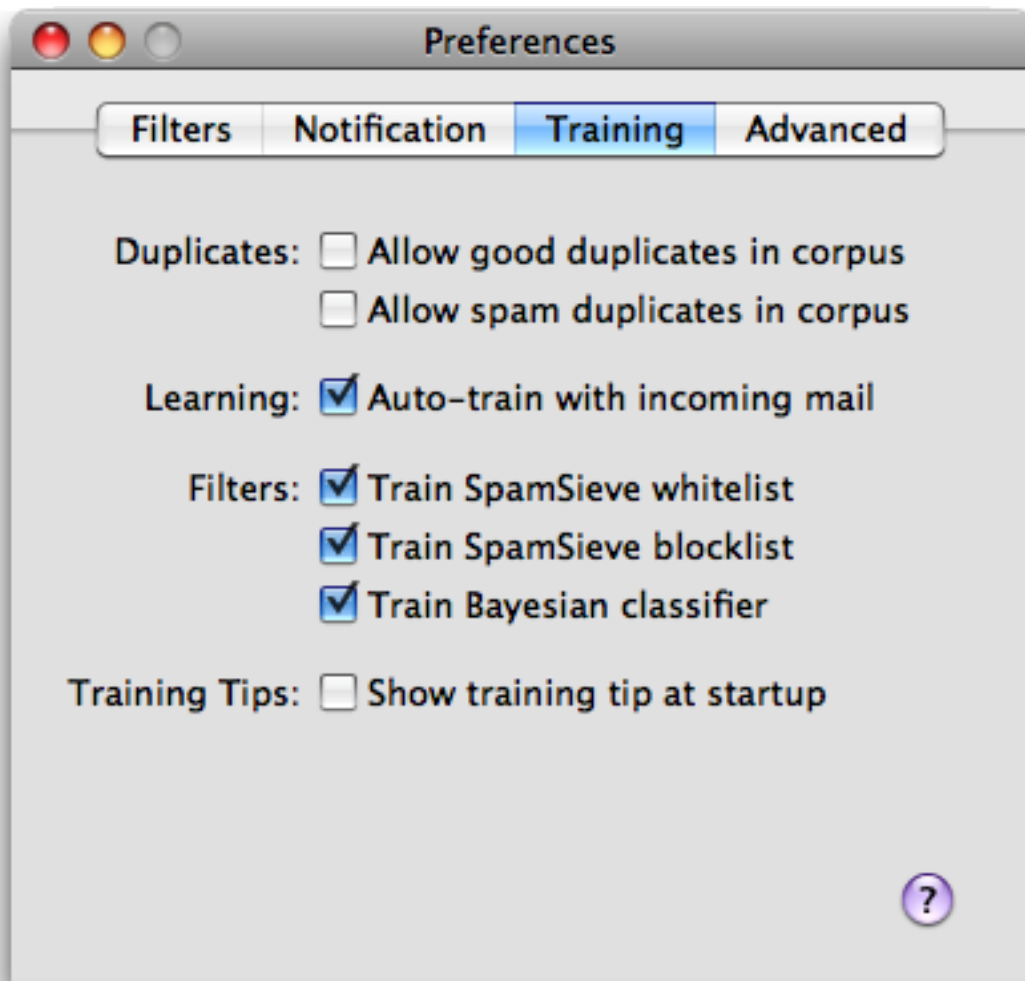
6.3.1   Allow duplicates in corpus

If you allow duplicate messages in the corpus, training SpamSieve with the same message twice will increase the corpus counts for the words in that message. If you do not allow duplicate messages, the second and subsequent trainings with that message will have no effect. By default, duplicate messages are not allowed in the corpus. This is nice because it means that you do not have to remember which messages you have already trained SpamSieve with; accidentally training with the same message more than once will not skew the data that you are providing to SpamSieve. If you wish to intentionally skew the data, you can check one or both boxes to allow duplicates.

6.3.2 Auto-train with incoming mail

This option causes SpamSieve to automatically train itself with newly received messages based on their predicted categories. Thus, after the initial training you would only need to train SpamSieve to correct its mistakes. It would automatically learn from the other new messages, as needed, trying to keep a proper balance of good and spam messages in the corpus. As the corpus increases in size, the rate of auto-training will automatically decrease to prevent it from growing too large.

Most SpamSieve users should keep auto-training on at all times. Reasons that you might turn it off include:

Testing Purposes

If you're trying to figure out why SpamSieve is processing a certain kind of message in a certain way, turning off auto-training reduces the interactions among SpamSieve's components and makes it easier to see what's happening.

Preventing Incorrect Training

When auto-training is enabled, it is imperative that you correct SpamSieve when it makes a mistake; otherwise it will "learn" things that aren't true and begin making predictions based on that incorrect information. If your mail program and filters are set up such that you cannot tell when SpamSieve has made a mistake (or if you can see the mistakes but sometimes forget to correct them), then you should not use auto-training.

Bulk Processing

For example, if SpamSieve will be processing a large number of incoming messages in a row, and you will not be able to correct any mistakes until later. In this case, using auto-training could magnify one or two mistakes into many, as SpamSieve would assume that it had classified the earlier messages correctly, and learned from that (possibly incorrect) assumption.

6.3.3 Train SpamSieve whitelist

With this option enabled, training SpamSieve with a good message will add the message sender's name and address to SpamSieve's whitelist. Training SpamSieve with a spam message will disable the name and address if they appear in the whitelist.

Example: You receive an Amazon order receipt and train SpamSieve with it as a good message. This puts `auto-confirm@amazon.com` on the whitelist so that future order receipts are always marked as good. A spammer might decide that `auto-confirm@amazon.com` would make a good fake return address. If you receive such a spam, SpamSieve would mark it as good because the sender was on the whitelist. If you then tell SpamSieve that the message is spam, it will disable the whitelist rule so that it can catch future spam messages with that return address.

6.3.4   Train SpamSieve blocklist

With this option enabled, training SpamSieve with a spam message will add the message sender's name and address to SpamSieve's blocklist. Training SpamSieve with a good message will disable the sender's name and address if they appear in the blocklist.

6.3.5   Train Bayesian classifier

With this option enabled, training SpamSieve with a message will add the words from that message to SpamSieve's corpus. It is highly recommended that you train the Bayesian classifier, as it is what SpamSieve uses to catch most spam messages.

6.3.6   Show training tip at startup

With this option enabled, SpamSieve will open the **Training Tip** window each time it is launched. If SpamSieve is hidden when it's launched, the window will not be opened, as that would unhide SpamSieve.

6.4 Advanced
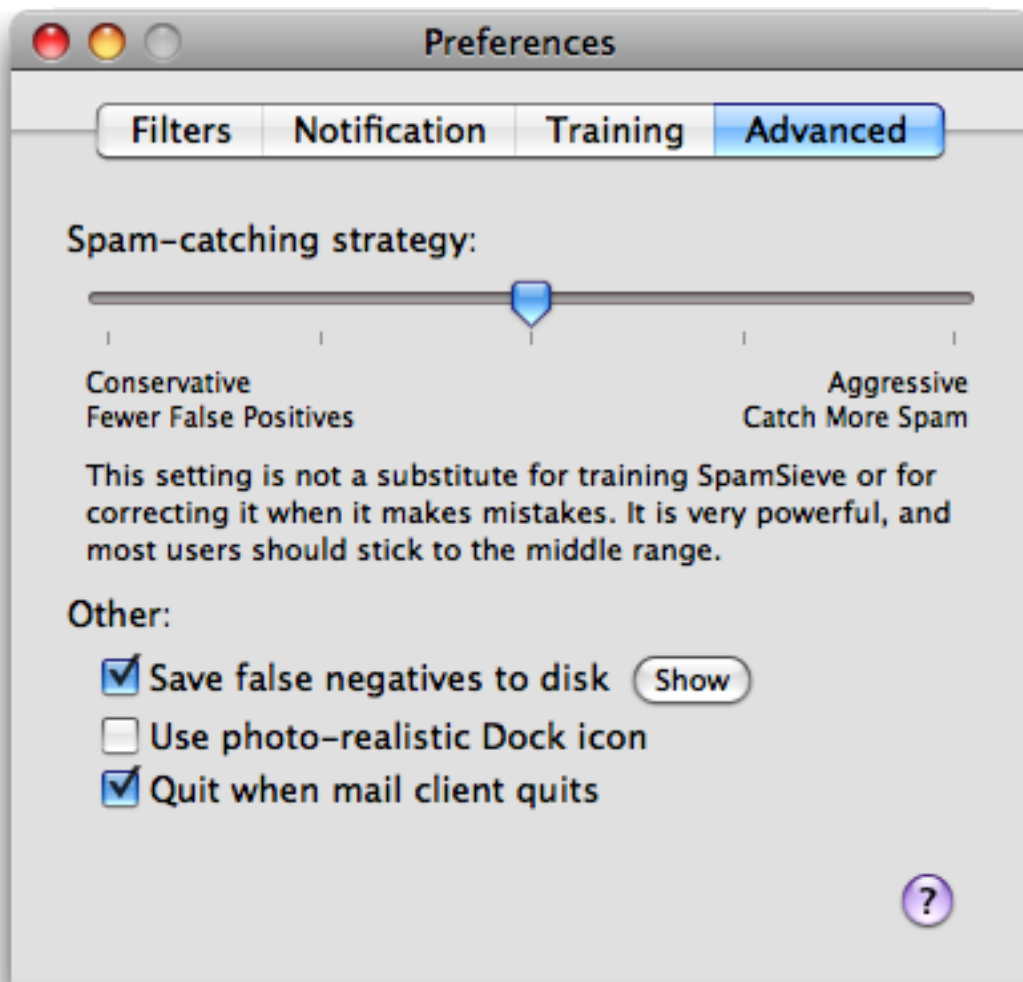
6.4.1 Spam-catching Strategy

This slider lets you adjust SpamSieve's bias. The bias controls how aggressive SpamSieve's Bayesian classifier is at catching spam. When SpamSieve is more aggressive, it is better at catching spam messages that share some characteristics with your good mail. When SpamSieve is more conservative, it will be better at marking borderline messages such as order confirmations and press releases as good. This setting is very powerful, and most users should stick to the middle range. It is also not a substitute for training SpamSieve or making sure that it's setup properly. Only change the bias if SpamSieve is consistently making errors in the same direction.

6.4.2 Save false negatives to disk

False negatives are spam messages that SpamSieve examined but didn't think were spam. This option causes SpamSieve to save such messages for later analysis. Clicking the **Show** button opens the folder containing the saved messages. You can e-mail this folder, or selected files from it, to spamsieve-fn@c-command.com[37]. By looking at the messages that SpamSieve missed, I can improve its algorithms to catch such messages in the future. Note that enabling this option will slow down SpamSieve's processing.

6.4.3 Use photo-realistic Dock icon

This option causes SpamSieve to use a more modern Dock icon, which may or may not fit in better with your other Dock icons.

6.4.4 Quit when mail client quits

With this checked, SpamSieve will quit itself when you quit an e-mail program, provided that there are no other mail programs running. This prevents SpamSieve's icon from filling up your Dock when it's not actually being used.

7   Frequently Asked Questions

7.1   Why is SpamSieve not catching my spam?

There are two basic causes of poor accuracy, setup problems and improper training:

Setup

SpamSieve itself may be working properly, but if it doesn't have access to your incoming messages, it won't be able to tell which ones are spam. First, check SpamSieve's log to see if SpamSieve is analyzing your messages or if you need to adjust its preferences. If SpamSieve is not analyzing your messages, you can check its setup by following these steps:

Apple Mail, Entourage, and PowerMail Setup

The setup processes for Apple Mail, Entourage, and PowerMail involves creating a *rule* in the mail program. When this rule is applied to a message, SpamSieve can examine its contents and send it to the spam folder (if it's spam). Make sure that you have a rule that looks exactly like the one in the SpamSieve manual.

---

[37]`mailto:spamsieve-fn@c-command.com`

To test that the rule works, select a spam message in your mail program. If you are using PowerMail, go to the **Mark as Spam** pane of the preferences and temporarily uncheck **mark it as good** at the bottom of the window. Use the **Train Spam** (Apple Mail or Entourage) or **Mark as Spam** (PowerMail) command to tell SpamSieve that it is spam. Drag this message to your inbox and select it again. Then manually apply the rule:

- In Apple Mail, choose **Apply Rules** from the **Message** menu. (This will apply all the rules so, for testing purposes, go to Mail's **Preferences** window and move the SpamSieve rule to the top of the rule list.) The rule worked if the message moved to the spam folder.

- In Entourage, change the category of the message to **None**. Then choose **Apply Rule ▷ SpamSieve - Move If Spam** from the **Message** menu. The rule worked if the message moved to the spam folder (or, for IMAP/Exchange messages, if the category was changed to **Junk**).

- In PowerMail, choose **Perform Filter ▷ Spam: evaluate** from the **Mail** menu. Then choose **Open Log** from the **SpamSieve** menu. The rule worked if the last entry in the log says `Predicted:  Spam` and shows the subject for the message that you had selected.

If the rule worked, then the problem is that another rule (above it in the list) is preventing the SpamSieve rule from being applied. Dragging the SpamSieve rule higher in the list should help, as this gives the SpamSieve rule priority. In Entourage, Mailing List Manager rules are implicitly higher than the regular rules, and they can often interfere with the regular rules, even if it looks like they wouldn't. Try unchecking **Do not apply rules to list messages** in the **Advanced** tab of each Mailing List Manager rule, or delete the Mailing List Manager rules and re-create them as regular rules.

If the rule did not work, see below for how to fix it:

Fixing the Apple Mail Rule

- Make sure that SpamSieve's training commands appear in Apple Mail's **Message** menu. If you don't see them there, then try re-installing SpamSieve's Apple Mail plug-in and re-launching Apple Mail.

- Make sure that the rule's name starts with **SpamSieve**.

- If SpamSieve is no longer working (but was working previously), try quitting Mail and then using the **Install Apple Mail Plug-In** command in the **SpamSieve** menu. Often, this is all you'll need to do to get it working again.

Fixing the Entourage Rule

- Make sure that your rule is of the proper type. That is, if you have a POP account, you need a POP rule; if you have an IMAP account, you need two IMAP rules.

- Try installing fresh copies of the scripts. To do this, choose **Install Entourage Scripts** from the **SpamSieve** menu, and let it replace the existing files. Then go to Entourage's **Rules** window and delete and re-create the SpamSieve rule.

Fixing the PowerMail Filter

- The filter might be configured such that it excludes most messages from spam filtering. Try editing the **Spam: evaluate** filter so that it has just a single condition that says **Always**.

- Quit PowerMail, then delete the folder:

  `/Users/<username>/Library/Application Support/PowerMail`

  and then re-launch it. (If the script files that PowerMail uses to communicate with SpamSieve may be damaged, this will fix them.)

Eudora Setup

- Make sure that you see SpamSieve's plug-in (and no other junk/spam plug-ins) listed when you choose **About Message Plug-Ins** from the **Eudora** menu.

- Make sure that the **Junk Threshold** is set to 50 and **Hold junk in Junk mailbox** is checked in Eudora's **Junk Mail** settings.

- Make sure that **Run junk scoring plugins on this IMAP account** is checked in Eudora's **IMAP** settings (if you have an IMAP account).

- Make sure that **Mail isn't junk if the sender is in an address book** in Eudora's **Junk Mail** pane is not checked.

Mailsmith Setup

- Make sure that **Use SpamSieve** is checked[38] in the preferences.

- If you are using **Leave it in "(incoming mail)"**, make sure that a deposit or transfer filter isn't acting on the spam messages before your spam filter can.

Thunderbird Setup

- Make sure that **Do not mark mail as junk if the sender is in**. . . is not checked.

- Make sure that **Trust junk mail headers set by**. . . is not checked.

Spam Messages From Your Address

If the missed spam messages have your own e-mail address in the "From" line, make sure that you check SpamSieve's Exclude my addresses option, and that you have used the Update Address Book "Me" Card command.

Training

SpamSieve is nearly 100% accurate, but only when properly trained. For best results, the corpus should have about 65% spam messages, as shown at the bottom of the **Statistics** window. You can manually train SpamSieve with more messages to improve this ratio, or let it auto-train itself with incoming messages.

The messages in the corpus should be representative of the messages that you receive. Adding more messages to the corpus generally improves accuracy, but it is not necessary to have more than a few thousand messages in the corpus (and having more than that will probably *reduce* accuracy). If the corpus is very large or very unbalanced, and there are so many messages in it that you cannot get it close to the 65% ratio, then you should reset the corpus and re-train SpamSieve. For more information, see this section.

---

[38]`http://www.barebones.com/support/faq/faq.php?action=question&minor_id=9&question_id=117`

7.2 Why is every message going to the Spam mailbox?

Apple Mail

Make sure that you have installed SpamSieve's Apple Mail plug-in. The name of the Spam-Sieve rule in Apple Mail must begin with "SpamSieve". Make sure that there are no leading spaces in the name. If the rule name does not begin with "SpamSieve", Mail will move every message to the **Spam** mailbox without even showing the messages to SpamSieve.

Entourage

Make sure that you've disabled Entourage's built-in Junk Mail Filter and that the SpamSieve rule(s) in Entourage are setup exactly as shown[39].

7.3 What information should I include when I report a problem?

Make sure that your message says which versions of Mac OS X and SpamSieve you are using, as well as the name and version of your mail program.

If the problem concerns SpamSieve's training or its accuracy, please attach the log file:

```
/Users/<username>/Library/Logs/SpamSieve/SpamSieve Log.log
```

to your message. That is, the file is called `SpamSieve Log.log`, and it is located inside the `SpamSieve` folder in the `Logs` folder in the `Library` folder that's in your home folder. (In most cases there's no need to attach the old, dated log files, whose names end with `.log.bz2`.)
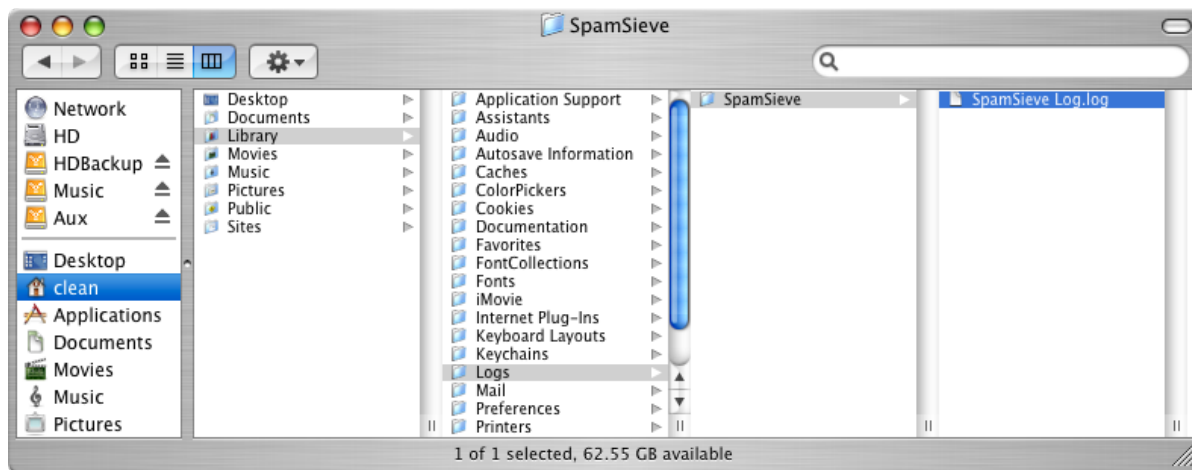
If you are reporting spam messages that SpamSieve didn't catch, please do not forward the messages using your mail program. Instead, enable the Save false negatives to disk preference so that SpamSieve will save future such messages to the folder:

---

[39]http://c-command.com/spamsieve/manual-ah/installing3

```
/Users/<username>/Library/Application Support/SpamSieve/False Negatives/
```

Then send the files in this folder to spamsieve-fn@c-command.com[40] as an attachment. If, after enabling the preference, a spam message gets through and is *not* saved in the `False Negatives` folder, this likely means that there is a setup problem and SpamSieve was not given an opportunity to filter that message.

If the problem concerns SpamSieve's setup and interaction with your mail program, please include relevant screenshots of the SpamSieve rule, the rules list, or the message list. To take a screenshot, hold down the Apple and Shift keys and press the number 4. Then use the mouse to select the area of the screen that you want to take a picture of. This will create a file called `Picture 1` on your desktop. Pressing the keys again will create `Picture 2`, etc.

7.4 How can I copy my training data to another machine?

SpamSieve stores its training data in the folder:

```
/Users/<username>/Library/Application Support/SpamSieve/
```

and it stores its preferences in the file:

```
/Users/<username>/Library/Preferences/com.c-command.SpamSieve.plist
```

To transfer SpamSieve's data to another machine, first quit both copies of SpamSieve. Then copy the folder and the preferences file to the corresponding locations on the other machine.

7.5 Why doesn't my serial number work?

You need to enter the *serial number name* and *serial number* exactly as they appear on your order confirmation e-mail. If you no longer have this e-mail, you can look up the name and number. Launch SpamSieve and choose **Purchase** from the **SpamSieve** menu. Then click the **Lost Your Serial Number?** button.

7.6 How can I hide SpamSieve's Dock icon?

The easiest way is to use the free Dockless[41] utility: wait for Dockless to generate a list of your applications, find SpamSieve in the list, uncheck the box next to it, and quit. When SpamSieve's

---

[40]mailto:spamsieve-fn@c-command.com
[41]http://homepage.mac.com/fahrenba/programs/dockless/dockless.html

Dock icon is hidden, its menubar is inaccessible, but a new command called **SpamSieve - Open Window** will appear in Apple Mail's **Message** menu after quitting and relaunching Apple Mail. This lets you configure SpamSieve's preferences, view the statistics, and access other parts of SpamSieve's user interface. With other mail programs, you will need to use this script[42] in order to do that.

Alternatively, you can do this manually. Hold down the Control key and click on the SpamSieve icon in the Finder. Choose **Show Package Contents** from the menu. Open the `Contents` folder, and then open the `Info.plist` file using TextEdit. At the bottom of `Info.plist`, change:

```
<key>LSUIElement</key>
<string>0</string>
```

to:

```
<key>LSUIElement</key>
<string>1</string>
```

(That is, just change the `0` to `1`.) Then save the `Info.plist` file and relaunch SpamSieve. You may need to temporarily move the SpamSieve application to the desktop and double-click it there in order for Mac OS X to notice that you now want the Dock icon hidden. To make SpamSieve's Dock icon visible again, change the `Info.plist` file back; that is, change the `1` back to `0`.

If you download a new copy of SpamSieve, it will have a new `Info.plist` file, so you would need to make the above change again if you still want SpamSieve's Dock icon to be hidden.

7.7   Can I use SpamSieve with more than one mail program at a time?

Yes; many people do this to separate their personal and business mail, and you can even use the two mail programs simultaneously. You just need to follow the setup instructions once for each mail program. SpamSieve will share its training data, rules, and statistics among all the mail programs.

7.8   Why doesn't SpamSieve launch when I open my mail program?

This is probably normal. SpamSieve only launches automatically when there is new mail to be processed, or when you train it. Of course, you can manually launch SpamSieve at any time or make it a startup item.

---

[42]http://c-command.com/scripts/spamsieve/open-window

7.9 How can I use SpamSieve with AOL?

There are three ways:

- AOL has recently announced support for IMAP. This means that you can check your AOL mail—and use SpamSieve to filter it—using e-mail programs other than AOL's own. I recommend using Apple Mail, since it has the best IMAP support among the mail programs that work with SpamSieve. You should configure[43] Mail using your AOL screen name and password. Set the IMAP server to `imap.aol.com` (port 143) and the SMTP server to `smtp.aol.com` (port 587).

- If you already have a copy of Claris Emailer, you can configure it to access your AOL account and filter the mail using SpamSieve.

- You can use a utility such as Mail Forward[44] to forward your AOL mail to a POP account. Then you can download the messages using *any* of the e-mail programs that SpamSieve supports.

7.10 How does SpamSieve compare with Eudora's SpamWatch?

Although they use similar technology, SpamSieve's Bayesian classifier is more accurate and learns more quickly than SpamWatch. SpamSieve is also more customizable. For instance, it can use whitelist and blocklist rules in addition to using the Bayesian classifier. If you look at the Filters tab of SpamSieve's Preferences window, none of the items above Use Bayesian Classifier are supported by Eudora. Lastly, SpamSieve can work with the Sponsored (free) Eudora, while SpamWatch requires the Paid ($50) version of Eudora.

7.11 Why don't I see the Junk command in Eudora's Message menu?

The Eudora installation instructions show how to enable this command from the esoteric settings.

7.12 Where can I download the older Mac OS 9 version?

There has never been an OS 9 version of SpamSieve—sorry.

---

[43]`http://help.channels.aol.com/article.adp?catId=1&sCId=416&sSCId=4093&articleId=217449`
[44]`http://www.sspi-software.com`

7.13 Can I delete spam messages after training SpamSieve with them?

Yes. It is not necessary to keep the spam messages in your e-mail program's spam folder because SpamSieve stores the information that it has extracted from the messages elsewhere.

7.14 What is the difference between Train Spam and Move If Spam?

The **Train Spam** command causes SpamSieve to learn from the selected messages. SpamSieve learns that they are spam, and then it moves the messages to the **Spam** folder in your e-mail program.

The **Move If Spam** command asks SpamSieve to *predict* whether the messages are spam. If it thinks that they are, it will move them to the **Spam** folder. Generally, you do not need to use the **Move If Spam** command directly; it will be automatically applied to incoming messages by the rule that you created in your e-mail program.

8 Legal Stuff

Distribution

Please distribute the unmodified `SpamSieve-2.7.dmg` file on the Web, LANs, compilation CD-ROMs, etc. You may not charge for it (beyond a reasonable cost for media) or distribute the contents of the disk image file in isolation. You may not distribute your serial number.

Limited Warranty

The software is provided "as is," without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use or other dealings in the software.

License

A license for SpamSieve is good for one person *or* one computer. You may install it on one Mac, and everyone sharing that Mac may use it (on that Mac). Alternatively, you may install it and use it on multiple Macs (e.g. your desktop Mac and your laptop); then you (and no one else) may use it on any of those Macs. For multiple users on multiple Macs, you should purchase multiple licenses.

Copyright and Trademarks

Components

The following open-source components are used in SpamSieve:

- Regular expression support is provided by the PCRE[46] library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

- Core Foundation[47] is available under the terms of the Apple Public Source License[48].

- Growl[49] is Copyright © The Growl Project, 2004-2007 All rights reserved.

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

  2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

  3. Neither the name of Growl nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

[45]mailto:mjt@c-command.com
[46]http://www.pcre.org
[47]http://www.opensource.apple.com/darwinsource/10.4.10.x86/CF-368.28/
[48]http://www.opensource.apple.com/apsl/
[49]http://growl.info

- Thanks to Allan Odgaard for some code snippets that are used in the Software Update installer.

- EDCommon[50] is Copyright © 1999—2002 by Erik Doernenburg. All rights reserved. Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation, and that credit is given to Erik Doernenburg in all documents and publicity pertaining to direct or indirect use of this code or its derivatives.

- EDMessage[51] is Copyright © 2000—2002 by Erik Doernenburg and Axel Katerbau. All rights reserved. Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation, and that credit is given to Erik Doernenburg in all documents and publicity pertaining to direct or indirect use of this code or its derivatives.

9 Version History

2.7—May 21, 2008

- Now requires Mac OS X 10.4 or later.
- Made a variety of accuracy improvements, focused on dealing with obfuscations, image attachments, URLs, and HTML.
- Improved corpus speed and memory use.
- Made various improvements to the column widths and alignments in the rules and corpus windows, and added alternating row colors.
- Fixed a rare problem where Apple Mail on Mac OS X 10.5 might hang if you trained a message as spam while Mail was downloading messages.
- If the OS reports an error when playing a sound as an alert sound, SpamSieve now plays it using the normal sound channel.
- Increased the range of possible values for the uncertain spam threshold.
- Improved sorting of sound names in the pop-up menu.
- Fixed bug where SpamSieve wouldn't launch if the `Microsoft User Data` folder had been replaced by an alias file that was invalid.
- No longer shows the **Reset Corpus/History** alert at launch if you hold down other modifier keys in addition to Command-Option.
- Updated the Dutch localization.

---

[50] http://www.mulle-kybernetik.com/software/EDFrameworks/download.html#EDCommon
[51] http://www.mulle-kybernetik.com/software/EDFrameworks/download.html#EDMessage

2.6.6—January 23, 2008

- Made various accuracy improvements.
- Rewrote internal corpus storage to work around a performance bug in Mac OS X 10.5 that could, in some circumstances, make SpamSieve very slow to launch.
- Worked around a problem on Mac OS X 10.5 where the Apple Mail plug-in would sometimes try to launch multiple copies of SpamSieve (and then they'd all self-quit, leading to -609 errors).
- Made some internal changes so that Use Growl global notification system works more reliably on Mac OS X 10.5.
- The Flash PowerMate notification feature now works with version 2.1 of the PowerMate software.
- If SpamSieve's corpus file or history database is damaged, you can now hold down the Command and Option keys at launch to reset them.
- Growl notifications are now posted from a background thread, to speed up message filtering.
- Fixed bug where the open panel for the Import Addresses. . . command was slow.
- Worked around a problem that could cause corruption of SpamSieve's Entourage scripts.
- Fixed rare crash when processing HTML messages.
- If SpamSieve is unable to install its Apple Mail plug-in, it now does a better job of helping you complete the installation manually.
- Integration with Apple Mail and Entourage no longer relies on the `mydefaults` command-line tool, since it had some limitations and there were occasional problems installing it.
- The software updater is better at handling invalid downloads folders.
- Added Dutch localization and updated the other localizations.

2.6.5—November 14, 2007

- Now requires Mac OS X 10.3 or later.
- Made various accuracy improvements.
- Added high-resolution version of the application icon.
- Adjusted the appearance of the status indicators (•, G, S) for better visibility in the Leopard Dock.
- Updated the default whitelist rules.
- Updated documentation for Mac OS X 10.5.
- Updated to PCRE 7.4.
- Improved compatibility with pre-release versions of Entourage 2008.
- The **Train as Good** command in Apple Mail now recognizes spam mailboxes whose names *end* with "Spam", and it works with the Trash mailbox on Mac OS X 10.5.
- Worked around change in Apple Mail on Mac OS X10.5 that could cause the **Train as Spam** command not to move the messages.

- Fixed bug where the Apple Help didn't work on Mac OS X 10.5.
- Fixed hang processing some pathological HTML spams.
- Fixed bug where Growl notification preferences got reset if you ran SpamSieve under different localizations.
- Fixed unnecessary Console logging when loading Entourage addresses.
- Updated Italian localization.

2.6.4—August 20, 2007

- Made more accuracy improvements for messages with attachments.
- Fixed a bug that could cause crashes when processing messages containing PDF attachments.
- Updated localizations.

2.6.3—August 3, 2007

- Made various accuracy improvements, particularly for messages with attachments.
- Improved compatibility with pre-release versions of Mac OS X 10.5 Leopard.
- Fixed bug where the Software Update checker didn't always re-check for new updates.
- Restored progress bar when loading Entourage addresses.
- Updated the localizations.
- Improved the documentation.
- Fixed help book icon.

2.6.2—May 4, 2007

- Made changes to prevent a crash on Mac OS X 10.4.9 when quitting in response to a mail program quitting.
- Slight changes for better accuracy.
- Fixed regression where the Import Addresses. . . command didn't always work for text files in the default encoding.
- Blocklist and whitelist rules that use **Body (any text part)** can now match text from the headers of bounced messages (which e-mail clients often display as part of the message body).
- The Software Update feature now checks whether the updated version can run on your installed version of Mac OS X.
- Better logging of messages that don't have a sender.
- Fixed a threading bug.
- Made an optimization to the Apple Mail plug-in.
- Adjusted the setup instructions for Apple Mail to avoid problem with the Previous Recipients list.
- Modernized the crash reporter code.

- Updated the French and German localizations.

2.6.1—April 9, 2007

- Fixed regression where SpamSieve wouldn't launch if you had a large number of Mac OS 9 sound files.
- Fixed bug where Thunderbird messages that were manually marked as junk weren't moved to the junk folder. If you are using Thunderbird, first update to SpamSieve 2.6.1, then choose **Install Thunderbird Plug-In** from the **SpamSieve** menu to update the plug-in.
- Made change prevent crash on Mac OS X 10.4.9 when quitting in response to a mail program quitting.

2.6—March 19, 2007

- SpamSieve now works with Mozilla Thunderbird.
- Improved detection of image spams and phishing messages.
- Made various message analysis improvements to increase the accuracy of the Bayesian filter.
- AppleScripting the whitelist and blocklist is much more efficient for scripts that access a lot of rules.
- Improved compatibility with pre-release versions of Mac OS X 10.5 Leopard.
- When installing a plug-in for a mail program, SpamSieve now opens the relevant page of the Apple Help to help you complete the installation.
- The alert when SpamSieve has auto-updated its Apple Mail plug-in is now non-modal, so it doesn't interfere with spam filtering.
- The Software Update checker now works behind an HTTP proxy, and the auto-updater is now compatible with FileVault.
- Can now import addresses from the incorrectly encoded .vcf files that are generated by recent versions of Address Book.
- Growl notifications are now enabled by default.
- The Apple Mail plug-in is more robust.
- Fixed some small memory leaks.
- Made some performance optimizations to the message tokenizer.
- SpamSieve is more robust when processing incomplete messages.
- The Entourage "Train Good" command now moves messages out of the **Uncertain Spam** folder.
- The Apple Mail "Train as Good" command now moves messages out of **zSpam** mailboxes.
- Updated to PCRE 7.0.

2.5—October 30, 2006

- Made lots of changes to the parser and classifiers to improve accuracy, especially for HTML and image messages.
- The in-memory corpus representation is much more efficient, which should lead to lower memory use and greater speed.
- Rewrote the Software Update feature. When a new version is available, it can now show you the release notes. SpamSieve now downloads the new version itself, rather than relying on your browser. On 10.3 and later, the **Download & Install** button will cause SpamSieve to auto-update itself to the latest version.
- Improved accuracy on messages containing misspelled words.
- Now requires Mac OS X 10.2.8 or later.
- Auto-training now places a higher priority on corpus balance compared to learning from novel messages.
- Improved the Apple Mail plug-in's **Train as Good** script to work around a bug in Mail.
- Improved the reliability of the Apple Mail training commands.
- Made further changes to improve the success rate of the Apple Mail plug-in installer.
- Updated to PCRE 6.7.
- Entourage training progress messages no longer block if Entourage is in the background.
- Worked around OS bug that prevented the **Statistics** sheet from properly parsing dates when the user's date format started with a two-digit year.
- No longer quits with an internal error if the `mydefaults` tool can't be installed.
- Added keyboard shortcut for **Hide Others**.
- Fixed bug with Purchase window sheet.
- Removed some old, unused code.
- Updated the toolbar icons.
- Various localization and documentation improvements.
- Fixed bug with display of remaining demo time.
- The Entourage script installer is more robust when contacting Entourage via AppleScript fails.
- Improved compatibility with Leopard.
- The date in the Statistics window more closely matches the user's preferences (10.4 and later).
- Better at detecting damaged corpus files (instead of crashing).
- Fixed bug where Uncertain Spam growls were always sent, even if disabled in SpamSieve's preferences.
- Adjusted workaround for Help Viewer bug.
- Increased the maximum width of the Hits column in rule list windows.
- Added thousands separators throughout the Statistics, Corpus, and rules windows.
- Fixed bug where adding a rule didn't create a new rule if there was already a rule with a blank "Text to Match."

- Fixed rare crashing bug when performing operations during idle time.
- Removed the Import Messages command (which let you train SpamSieve directly from a file in mbox format), because there are now very few situations where it is useful, and it was confusing people.
- Added screenshot showing where to find Entourage scripts.

2.4.4—July 13, 2006

- Made various changes to improve SpamSieve's accuracy, particularly when processing blank messages, HTML messages, and messages containing images.
- The following strings may now be used in rules to match headers that are missing: `<SpamSieve-Unknown-Subject>`, `<SpamSieve-Unknown-From>`, `<SpamSieve-Unknown-FromName>`, `<SpamSieve-Unknown-To>`. It is somewhat common for messages to have a blank subject (which can be matched using the empty string), but legitimate messages that omit the Subject for From header are rare, and now these can easily be matched by creating the appropriate rules on the blocklist.
- Quit when mail client quits is now enabled by default.
- Log entries are now abbreviated when the string that matched the rule is long.
- The Apple Mail **Train as Good** command can now move messages out of submailboxes of the **Junk** mailbox.
- The Apple Mail plug-in installer works better when the folder permissions are messed up.
- Can now auto-recover from damaged message store files, rather than complaining to the user about them.
- If SpamSieve is hidden when launched, it will refrain from opening the **Training Tip** window.
- Improved the documentation, training tips, and localizations.
- Various code modernization and bullet-proofing throughout.
- Fixed localization bugs that could cause crashes.
- Fixed crash when hiding the progress panel.
- Fixed crash when saving false negatives to disk.
- Made changes to the Entourage scripts to try to work around an OS bug that causes them to grow and eventually become corrupted.
- Worked around OS bug to prevent freezes when attempting to play damaged sound files.

2.4.3—March 30, 2006

- Improved SpamSieve's accuracy by counteracting various spammer tricks.
- Removed the delay, when using Apple Mail on Tiger, between choosing "Train as Good" or "Train as Spam" and when training actually started.

- The Entourage scripts now report progress part way through bulk trainings and allow you to cancel. They also warn if it looks like you're training SpamSieve with too many messages, and they're better at preventing duplicate categories from being created in Entourage. The "Train Spam" script now removes the spam messages from the server.

- Growl notifications from people in the address book now include the "To" address for mailing list messages. This makes it easier to decide whether to ignore the notification.

- Fixed bug that caused part of SpamSieve's corpus to be written to disk incorrectly when running on Intel. In most cases, no ill effects would have been observed, and SpamSieve will repair the corpus file the first time you launch 2.4.3.

- Improved the error messages.

- Improved the display of the demo time remaining.

- Updated the localizations.

2.4.2—February 23, 2006

- SpamSieve is now much better at catching a new type of spam message that previous versions had been inconsistent at catching.

- Worked around some more spammer tricks to improve accuracy.

- Improved the way message attachments are analyzed.

- Fixed bug that could cause improper analysis of messages from Apple Mail or Eudora, leading to reduced accuracy.

- Improved phish detection.

- Improved the performance of the Apple Mail training commands on Tiger and Jaguar.

- Made some changes to the way spam messages are colored in Apple Mail. Now, the most spammy color (blue) is reserved for messages with scores 99 or higher, i.e. messages that matched a blocklist rule, had encoded HTML parts, or were known to definitely be spam.

- The **Show Window** command in Apple Mail can now open the SpamSieve help.

- Under certain circumstances, SpamSieve can now detect at launch whether the application package is damaged, rather than too-quietly reporting errors in the log during message processing.

- Improved the troubleshooting documentation.

- Updated the Japanese localization.

2.4.1—January 25, 2006

- SpamSieve is now a universal binary[52].

- Made various changes to SpamSieve's tokenizer and HTML parser to improve accuracy.

- Improved filtering of messages containing attachments.

- Added Apple Mail settings to control whether messages trained as spam are marked as read and/or left on the server.

---

[52]http://www.apple.com/universal/

- Better at finding notification sounds that are built into mail clients.

- Now shows uncertain growls when notification is suppressed.

- SpamSieve now delegates more file reveal operations to Path Finder 4, since it fixes a bug in Path Finder 3 that prevented certain reveals from working.

- Rather than typing (or copying and pasting) your name and serial number to personalize SpamSieve, you can now click the `x-spamsieve://` URL that's sent to you when you purchase[53] SpamSieve or get a serial number reminder[54].

- Fixed bug where the rules list would scroll one rule up if it was scrolled to the bottom and you edited a rule.

- Added Spanish localization and updated the Danish, Italian, Swedish, and Vietnamese localizations.

- Improved the installation and troubleshooting documentation.

- Removed spurious Section 4.4.1 of the manual.

2.4—November 16, 2005

- Made various changes to the Bayesian engine to improve accuracy.

- Added some heuristics for detecting phishes.

- Apple Mail messages can now be filed into different mailboxes based on how spammy they are (requires 10.3 or 10.4).

- The Apple Mail plug-in is now a Universal Binary, so SpamSieve can be used on Intel-based Macs without running Mail in Rosetta.

- Added support for the new (non-haiku) Habeas headers.

- SpamSieve now plays notification sounds using the alert volume rather than the master volume, and they'll be played on the same output device as alerts and sound effects. (The old behavior is still in effect when playing classic sound files and when running on Jaguar.)

- Added `suppressing notification` AppleScript parameter. You can use this to prevent SpamSieve from bouncing its Dock icon or showing Growls when recalculating the spam scores of old messages.

- The **Software Update** alert is now a sheet, so it won't interfere with spam filtering.

- If Path Finder is running, it will be used instead of the Finder to reveal files/folders.

- Made various tweaks to keep PowerMates from flashing when they shouldn't.

- Adjusted the standard set of rules.

- You can now tab back and forth between the search field and table in the corpus and rules windows (requires 10.4).

- `Predicted` entries in the log now show the message's sender.

- Added preference to control whether Apple Mail false positives are marked as unread.

---

[53]`http://c-command.com/store/`
[54]`http://c-command.com/sn`

- Added **Technical Support & Feedback** item to the **Help** menu.
- The Entourage scripts try even harder to avoid creating duplicate categories.
- SpamSieve now avoids loading the address book except when absolutely necessary. Thus, if your address book is corrupted such that loading it would cause a crash, you'll still be able to receive mail if you turn off SpamSieve's address book–related features.
- Messages with empty senders are no longer considered to be from people in the address book, even if the address book contains a contact with such an address.
- Fixed longstanding bug in which sorting the blocklist or whitelist by **Header** or **Match Style** would group the rules appropriately, but wouldn't order the groups alphabetically by the localized text in the column.
- Improved the error messages in the application and in the Apple Mail plug-in.
- Made a change to prevent Apple Mail from deadlocking (in rare circumstances) when training SpamSieve on Mac OS X 10.4.3.
- Fixed regression where `Trained:   (Auto)` log entries occurred before the corresponding `Predicted` ones.
- The Apple Mail training commands now respect the preference for whether to color messages.
- Added hidden preference `LogSpam` that you can turn on with `defaults write com.c-command.SpamSieve LogSpam YES` to make SpamSieve keep a maildir-style folder of the spam messages it's seen. Right now, this is not recommended for general use on slower machines.
- Updated link to Habeas Safelist.
- Updated eSellerate, PCRE, and SQLite libraries.
- Added Danish localization and improved the other localizations.
- Various documentation improvements, including:
  - Described how to place Entourage messages in different mailboxes based on how spammy they are.
  - Added section describing how to redirect non-spam Apple Mail messages to another account, e.g. to filter the mail that you receive on your Blackberry.

2.3.2—August 8, 2005

- Made various improvements to increase SpamSieve's accuracy.
- Added Quit when mail client quits option.
- Sped up filtering when Growl notifications are enabled. Improved the text/layout of the Growl notifications.
- Re-installing or updating Eudora could have the effect of re-enabling Eudora's built-in junk plug-ins. This could reduce the filtering accuracy and cause unexpected behavior as multiple plug-ins acted on the same messages. Now, if SpamSieve detects that its Eudora plug-in is installed, it will automatically disable any other Eudora junk plug-ins.
- When you reset the corpus, SpamSieve automatically creates a dated backup so that it's possible to revert, if need be.

- The pop-up menu for selecting the uncertainty threshold now supports scores as high as 98. This makes it possible to designate all non-blocklisted spam messages as uncertain.

- The S and G indicators are now only shown in the Dock icon after manual training, not auto-training.

- The log is now UTF-8 rather than ASCII, so it should be much more readable for people using localized versions of SpamSieve.

- More errors are now logged.

- Better at finding sound files that are built into Mailsmith.

- Worked around Tiger bug that would cause archived log files to not decompress automatically when opened.

- Fixed regression where SpamSieve could crash if you tried to install the Entourage scripts when Entourage was not installed.

- Fixed bug in Apple Mail's **Train as Good**, where it didn't always move messages out of the **Spam** mailbox if there were lots of recipients.

- Fixed Entourage **Train Good** script to not make a new **Uncertain Junk** category when one already exists (but Entourage says that it doesn't).

- Worked around AppleScript error that could occur when running Entourage scripts.

- The regex code is more bulletproof in the face of rare OS errors.

- Added better heuristic for determining which files SpamSieve can import addresses from. This should prevent some rare crashes.

- Updated the Habeas link in the **Preferences** window.

- The history database is more robust on Tiger.

- The **Purchase** window now makes it more clear when the serial number has been successfully entered. Merged the **Web Purchase**. . . and **Instant Purchase**. . . buttons.

- Adjusted the way the remaining demo time is displayed, as it led many people to believe that they had less than a month of total trial time.

- Improved training tips and the manual.

- Added French translation[55] of manual. Updated Vietnamese manual. Fixed regression where the Italian and Vietnamese manuals were inaccessible.

2.3.1—May 16, 2005

- Works with Apple Mail on Mac OS X 10.4.1. SpamSieve should automatically install a new copy of its Apple Mail plug-in the first time it's launched, but if it doesn't you can do so by choosing **Install Apple Mail Plug-In** from the **SpamSieve** menu.

- Various accuracy improvements.

- Renamed the Apple Mail training commands to **Train as Good** and **Train as Spam**.

- **Train as Spam** is much faster in Apple Mail on 10.4 when there are multiple messages selected.

---

[55]http://c-command.com/spamsieve/manual-fr/

- If SpamSieve's Dock icon is hidden, a new **SpamSieve - Open Window** command will appear in Apple Mail's **Message** menu. This lets you quit SpamSieve or access its windows and settings while its menu bar is hidden.

- Worked around Apple Mail bug so that **Train as Good** now moves spam messages out of Mail's **Spam** folder on 10.4, provided that SpamSieve had put them there.

- Reduced the maximum size of the Growl notification bubbles.

- Better at parsing malformed messages.

- The HTML parser is much faster with certain pathological spam messages that could previously drag parsing out for a minute or more.

- Worked around Entourage bug that could lead to the creation of multiple **Uncertain Junk** categories.

- SpamSieve no longer complains about the permissions on Apple Mail's `Bundles` folder if you're using a different mail program.

- Removed the **Prune Corpus** command. With auto-training being much smarter than in earlier versions, it's almost never advisable to prune, and improper pruning severely reduces accuracy.

- The demo reminder window updates the number of days remaining if you leave Spam-Sieve running for days or weeks at a time.

- Fixed bug that could cause a crash when using **Instant Purchase**.

- Worked around crash caused by bug in 10.2.

- Updated localizations.

2.3—April 25, 2005

- General
  - Works with Mac OS X 10.4 (Tiger).
  - Made lots of improvements to SpamSieve's parsers and tokenizer for better accuracy. To fully take advantage of this, you will need to reset SpamSieve's corpus and re-train it (e.g. with 300 recent good messages and 600 recent spams). However, this is certainly not required, and I expect that most people will opt for the simpler upgrade of just installing the new SpamSieve application.
  - Auto-training works better. SpamSieve is smarter about selecting which incoming messages to train itself with, so that it reaches a high level of accuracy sooner, and it is better at adapting to new types of mail that you receive.
  - Improved the training tips and the training section of the manual so that it's clearer what the best practices are.
  - When training the whitelist, SpamSieve will now create rules that match the addresses of the other recipients. This should reduce false positives from people who haven't previously sent you mail, but who correspond with the same people you do.
  - Added Update Address Book "Me" Card command.

- Scriptability

- – Added `selection` AppleScript property, which can be used to get the selected token infos in the corpus or the selected rules in the whitelist or blocklist window. One use of this is demonstrated in a script[56] that adds the addresses of the selected whitelist rules to the Address Book.
  - – Added AppleScript properties and commands to access SpamSieve's windows and log. One use of this is demonstrated in a script[57] that lets you open SpamSieve's windows if its Dock icon is hidden (and thus the menubar is inaccessible).

- Notification
  - – Added option to control whether Growl notifications contain excerpts of the message body.
  - – The new message count in SpamSieve's Dock icon is now auto-positioned.
  - – Fixed regression where dragging the slider to adjust the size of the number in the Dock icon didn't temporarily show the number so that you could preview the results.

- Apple Mail Integration
  - – Improved accuracy due to better decoding of Apple Mail messages.
  - – The commands for training SpamSieve from Apple Mail are now in Mail's **Message** menu, rather than in the **Scripts** menu. This lets you access those commands in the same way on 10.2 through 10.4, and you don't have to worry about changing the scripts around if you boot into a different version of the OS.
  - – The Apple Mail plug-in is faster at processing messages.
  - – If the Apple Mail plug-in is installed but disabled for some reason (e.g. a location switch or OS re-install), SpamSieve will automatically re-enable it (takes effect when you relaunch Mail).
  - – Worked around bug in Mail that could prevent Train Good or Train Spam from working properly when training multiple messages at once that were already in their final destination.

- Eudora Integration
  - – The installer no longer asks you to find Eudora except when absolutely necessary.
  - – The Eudora plug-in is now installed in the `Application Support` folder rather than inside the Eudora application package. Thus, it's no longer necessary to re-install the plug-in when updating Eudora, although you still may need to disable the SpamWatch and SpamHeaders plug-ins if updating Eudora re-enables them.
  - – Added a **Cancel** button to the alert that you get if Eudora is already running when you ask SpamSieve to install the Eudora plug-in, in case you don't want to quit Eudora at that time.

- Fixes and Tweaks
  - – The Apple Help is now multiple linked pages, rather than a single page, so you can now use Help Viewer's search box.
  - – Simplified the setup instructions in the manual, and added new sections on customization.

---

[56]http://c-command.com/scripts/spamsieve/whitelist-to-address-book
[57]http://c-command.com/scripts/spamsieve/open-window

- Improved duplicate message detection.
- Fixed bug where e-mail addresses were not always correctly parsed out of mail headers.
- Tweaked the format of `Trained` entries in the log.
- Worked around OS bug that could cause SpamSieve to freeze when installing AppleScripts.
- SpamSieve is better at following aliases and more tolerant of incorrect permissions when looking for its support files.
- Updated to eSellerate Engine 3.6.1.
- Improved serial number name entry.
- Various localization fixes.
- The **?** buttons in the **Preferences** window now open the specific help sections on Jaguar.
- Fixed longstanding unreported bug where you could launch multiple instances of SpamSieve if you were using Jaguar.

2.2.4—February 10, 2005

- Increased the speed of SpamSieve's message processing.
- Processing messages with Entourage is much faster. To realize the speed increase, re-install SpamSieve's Entourage scripts and let it replace the existing ones.
- Improved accuracy through better HTML and header processing. (It is not necessary to reset the corpus.)
- Colors to indicate spamminess in Apple Mail are now enabled by default.
- Can now play sounds (and bounce the Dock icon) when mail arrives, even if SpamSieve or a mail program is frontmost.
- Added option to Entourage's **Change Settings** to make all spam messages marked with category **Junk** instead of marking some of them with **Uncertain Junk**.
- Added more standard blocklist rules for non-Latin character sets.
- AppleScript errors complaining about not being able to find the SpamSieve application should be much less common now. If you do see such an error, asking SpamSieve to re-install the scripts for Apple Mail or Entourage (and letting it replace the existing scripts) should cure things.
- Improved name and serial number entry.
- The **Edit Log** command is no longer an alternate menu item.
- Can now load Entourage addresses when Launch Services can't find Entourage.
- The default classifier reports better scores.
- The behavior of the default classifier (if no rules or other classifiers match, and the Bayesian classifier is disabled) may now be changed by setting the `DefaultIsGood` default. Normally this is `YES`, but you can set it to `NO` to make SpamSieve treat all non-whitelisted messages as spam.
- Pruning now is recorded in the log.

- Updated the Russian localization.
- Added Swedish and Vietnamese localizations.
- Expanded and improved the manual.
- The Entourage scripts no longer mark messages with multiple copies of the same category.
- Fixed bug where SpamSieve would sometimes incorrectly think that it had made a mistake (if auto-training was on and the user had asked it to reclassify a message).
- Fixed bug in the `Change Settings` scripts.
- No longer reports an error when trying to reset an empty initial corpus.
- Fixed crash when quitting after resetting an empty corpus.
- Fixed bug where SpamSieve would crash when reading a damaged corpus file.
- Worked around OS bug that could cause crashes when creating the **Uncertain Junk** category in Entourage.
- Notification dismissal now works on Tiger.
- Apple Mail's scripts are now installed in the correct location when running on Tiger.

2.2.3—November 15, 2004

- Fixed bug where SpamSieve would complain of a permissions error at startup.

2.2.2—November 14, 2004

- Can Notify with Growl when good messages arrive, and to help spot false positives without looking through the entire contents of the spam folder.
- Added **Change Settings** commands for Apple Mail and Entourage, which let you configure script options (spam folder name, behavior when using **Train Good** and **Train Spam**, etc.) without having to edit the scripts. The settings are stored in SpamSieve's preferences file, so they will persist if you update or re-install the scripts.
- Fixed bug where SpamSieve would report a syntax error when processing certain messages (typically in non-ASCII character sets).
- Better accuracy due to improved header and body analysis.
- Better accuracy due to smarter auto-creation of **From (name)** rules.
- Auto-training now takes scores into account; the corpus is updated using messages that were harder to classify, to forestall errors.
- Better handling of spam messages that lie about their encoding.
- Entourage now uses two separate categories for spam messages, so that you can see which ones are more (or less) spammy.
- Improved accuracy when processing messages in German.
- **Any Address** rules now match **SendTo** addresses.
- Better handling of messages with "From " lines.

- Worked around Mail performance problem where **Add Good** would hang if there were a lot of recipients.

- The Dock (and DragThing) good message counter no longer increases for messages received while the mail program is active.

- Added Russian localization.

- Improved the French localization.

- Better recovery from damaged `Rules` and `History.db` files.

- Added Italian-localized installation instructions.

- Improved launch time.

- Better parsing of PGP messages.

- Worked around 10.2 bug that could cause crashes when the **Training Tip** window was updated.

- Fixed bad interaction between auto-training and duplicates when the corpus was small.

- More tolerant of incorrect file and folder permissions.

- If Launch Services cannot find the Eudora application, the installer will now try some heuristics and prompt the user to locate Eudora, rather than giving up.

- The Apple Mail and Eudora plug-ins are better at finding and launching the SpamSieve application, and they will notify the user if they are unable to do this.

- Updated to eSellerate 3.5.9, which provides support for registration names using non-ASCII characters.

- When you type in your serial number, SpamSieve normalizes its spacing and case.

- The `Add Good` and `Add Spam` AppleScripts have been renamed `Train Good` and `Train Spam`. When installing the new scripts, SpamSieve will automatically move the old ones to the trash.

- The Entourage spam folder is now called **Junk E-mail** instead of **Spam**, since Entourage 2004 already has a so-named folder.

2.2.1—September 20, 2004

- Shows count of new good messages in [DragThing](#)[58] 5.3 and later, if you [install an integration script](#). (This script will be built into future versions of DragThing.)

- Fixed accuracy regressions from 2.1.4 and made some accuracy improvements.

- Added Italian localization.

- Auto-training will no longer add duplicate messages to the corpus, because they interfere with undo.

- You can now start a new paragraph in the crash reporter by pressing Return rather than Command-Return.

- Tries to add itself to the Launch Services database at launch, to make it easier for the scripts and plug-ins to find the SpamSieve application.

---

[58]http://www.dragthing.com

- Fixed bug where the help buttons in the **Preferences** window didn't work unless the main help had previously been opened.

- Improved the French and Japanese localizations.

- The **Edit Log** command will now open the log using an editor, rather than Console, if BBEdit is unavailable.

- Improved accuracy statistics when using Apple Mail IMAP accounts.

- The mailbox parser is faster and more tolerant of malformed mbox files.

- No longer tries to roll over the log more than once per day.

- Fixed regression where adding to the whitelist or blocklist didn't work if a disabled rule matched the message.

- Fixed crash that could happen when showing progress bar at launch.

- Fixed crash when scanning System 7–format sounds.

- Fixed bug where slightly spammy Apple Mail messages would be colored and recorded as spam, but not moved to the Spam mailbox.

2.2—August 24, 2004

- Accuracy Improvements
  - SpamSieve is smarter about what text to tokenize, it extracts more information from messages, it's better at detecting invisible text, and it can undo more spammer obfuscations.
  - The Bayesian classifier can leverage the results of SpamAssassin's heuristic tests. It also assigns better word probabilities and is better at deciding which parts of the message are important.
  - Messages containing Habeas headers are now checked against the Habeas Whitelist[59]. This protects against spam messages that include Habeas headers in order to get through filters.
  - Removed the **Import Seed Spam** command, as it would *reduce* accuracy with recent versions of SpamSieve.

- General Improvements
  - Auto-training is more automatic. There is now a single checkbox to enable auto-training and, if it's on, SpamSieve will try to do the right thing when it processes new messages. That is, it will train itself using messages of the types that it needs to see more of, and it will prevent the corpus from growing unbalanced or overly large. Also, it will update the whitelist using every incoming good message, so that you can have a complete whitelist without bloating the corpus.
  - The rules and corpus windows now have toolbars, and they support iTunes-style filter-searching.
  - The corpus and rules are now scriptable[60], and SpamSieve now supports AppleScriptKit terminology.

---

[59]http://c-command.com/aboutHabeas
[60]http://c-command.com/scripts/spamsieve/

- Assorted performance enhancements make SpamSieve faster and improve the responsiveness of its user interface.
- Added Portuguese localization.

- Blocklist and Whitelist
  - Rules support more match fields: **From (name)**, **Any Recipient**, **Any Address**, **Any Character Set**, and **Any Attachment Name**.
  - The new Import Addresses... command lets you import blocklist and whitelist rules from text files (e.g. address book exports or mbox files).
  - Added default blocklist rules for `.pif` and `.scr` attachments and a default whitelist rule for `lists.c-command.com`.
  - Rules can now match the empty string, e.g. when there is a subject header, but the subject is blank. They can also match absent headers by matching against, e.g. `<SpamSieve-Unknown-Subject>`.
  - The **Text to Match** field now abbreviates using an ellipsis if the text won't all fit.

- Notification
  - Can make a Griffin PowerMate[61] flash when new good messages arrive.
  - Now supports System 7–format notification sounds as well as Entourage sound sets[62]. In addition to the `Library/Sounds` folders, SpamSieve will now look for sounds installed with Apple Mail, Entourage, Mailsmith, and PowerMail.
  - Doesn't play the notification sound if you are using fast user switching and SpamSieve is running in one of the background sessions.
  - Notifications that require dismissal (continuous bouncing, PowerMate flashing) are no longer triggered when SpamSieve or the mail program is already frontmost. Thus, you don't have to deactivate the mail program and then activate it again to dismiss the notification.

- Apple Mail Integration
  - Sets the colors of spam messages to reflect how spammy they are, making it easier to skim the **Spam** mailbox for false positives.
  - Protects against Web bugs by telling Mail not to load the images from messages that are classified as spam.
  - The **Add Good** script is better at moving messages from the **Spam** folder back to the correct inbox, and it will mark them as unread when it does so.
  - The **Add Good** and **Add Spam** now work with Mac OS X 10.3.5.
  - The plug-in will look for SpamSieve in the `Applications` folder, even if Launch Services is confused and says it can't find it.

- Entourage Integration
  - The Exclude my addresses switch now also applies to the Entourage address book, to reduce the chances of a forged spam getting through.

---

[61]http://www.griffintechnology.com/products/powermate/
[62]http://www.soundsetcentral.com

- Added new scripting verb `add entourage addresses`. This will allow you to keep the Entourage addresses in sync[63] by using an Entourage shutdown schedule.
- Can automatically add the recipients[64] of the messages you send to the whitelist.
- Sanity-checks addresses that are loaded from Entourage. For instance, if both the name and the address were entered in Entourage's address field, SpamSieve will now extract just the address, rather than taking Entourage's word for it.
- The **Add Good** script now works with the Possible Spam[65] folder and marks false positives as unread.
- Messages can have more than one category, so SpamSieve now adds and removes the **Junk** category from the message, rather than *replacing* the category. This means that marking a message as junk doesn't wipe out other categories on the message.
- Shows a progress bar while importing Entourage addresses.

- Eudora Integration
    - Removed the option to use the full Eudora junk score range; this setting is now always in effect.

- Mailsmith Integration
    - Can automatically add the recipients[66] of the messages you send to the whitelist.

- PowerMail Integration
    - Can automatically add the recipients[67] of the messages you send to the whitelist.

- Statistics and Log
    - The **Statistics** window shows the number of blocklist and whitelist rules and the number of spam messages received per day. The date sheet has a **Now** button that enters the current date and time.
    - The log is now stored in `~/Library/Logs/SpamSieve`. The **Open Log** command now opens the log in Console, so that it's easier to monitor as it changes. To get the old behavior of opening the log in a text editor, hold down Option and choose **Edit Log**.
    - If the log file grows larger than 5 MB, SpamSieve compresses it, archives it by date, and starts a new log.
    - When SpamSieve makes a mistake, the log records which classifier made the error and what the message's score was. The log also now records parse errors and the number of messages in the corpus.

- Fixes and Tweaks
    - SpamSieve can optionally show an alternate, more photo-realistic, icon in the Dock.
    - There is a new mailing list[68] for discussion of SpamSieve.

---

[63] http://c-command.com/scripts/spamsieve/entourage-load-addresses
[64] http://c-command.com/scripts/spamsieve/entourage-whitelist-recipients
[65] http://c-command.com/scripts/spamsieve/entourage-separate-by-score
[66] http://c-command.com/scripts/spamsieve/mailsmith-whitelist-recipients
[67] http://c-command.com/scripts/spamsieve/powermail-whitelist-recipients
[68] http://lists.c-command.com/listinfo.cgi/spamsieve-talk-c-command.com

- Each tab of the **Preferences** window now contains a help button that will open the corresponding section of the Apple help.
- Updated to PCRE 4.5 and SQLite 2.8.15.
- Fixed bug where SpamSieve could crash when generating a messages's identifier if a system routine failed.
- Fixed bug in EDMessage that could cause crashes when decoding certain quoted-printable messages.
- Better handling of 8-bit subjects with no specified encoding.
- Worked around Panther bug that could cause crashes or drawing artifacts on the desktop by no longer trying to draw on the Dock icon when it's hidden.
- Worked around OS bug that prevented certain notification sounds from playing.
- Fixed bug where the selection was not always preserved when editing blocklist and whitelist rules.
- The **Show Corpus**, **Show Statistics**, and **Preferences**... commands in the Dock menu now bring SpamSieve to the front.
- The progress window when exporting the corpus sometimes lagged a bit before closing automatically.
- Fixed bug where SpamSieve would get confused if you entered the empty string as a date.

2.1.4—April 15, 2004

- Fixed bug where SpamSieve could crash when installing the Eudora plug-in if you were using Eudora 6.0.x.
- Fixed regression where SpamSieve couldn't process certain messages, resulting in a script error and reduced accuracy.
- Added French localization.
- Updated AOL instructions, since AOL now supports IMAP.

2.1.3—April 13, 2004

- Added menu commands for installing the Apple Mail plug-in and scripts, the Eudora plug-in, and the Entourage scripts. These items are now stored inside the SpamSieve application package.
- Scripts for the other applications are now stored inside the application bundle, not at the root of the disk image. The **Show Other Scripts** menu command will reveal them in the Finder.
- Apple Mail and Eudora users should update their plug-ins, using the commands in the **SpamSieve** menu.
- Added the `score` script command, which returns an integer between 0 and 100 indicating how spammy the message is. 50 and higher mean spam.
- The `Predicted` lines in SpamSieve's log now show the scores of the messages.
- Can now use Eudora's full 0-to-100 junk score range if you check the appropriate box in the **Advanced** preferences.

- Improved parsing of messages with 8-bit transfer data.

- Faster at processing messages.

- Added support for Outlook Express 5.

- Worked around OS bug that could cause SpamSieve to come to the front each time a message was processed in Apple Mail or Eudora (usually if an X11 application was frontmost).

- Fixed bug where errors encountered while processing messages were not reported in the log.

- Worked around Cocoa problem where certain notification sounds wouldn't play.

- Made the **Purchase** window easier to understand, and added a button for looking up lost serial numbers.

- Trims the text in the serial number field so people don't accidentally paste the number in twice.

- Software updater is better at checking whether the computer can connect to the Internet.

- SpamSieve now tries to parse Eudora messages according to RFC822, even though this will sometimes fail, as many Eudora messages are not RFC822-compliant.

- Adjusted the list of headers that SpamSieve ignores.

- Added keyboard shortcuts for Apple Mail scripts.

- Improved the training tips.

- Updated to SQLite 2.8.13.

- Updated to eSellerate SDK 3.5.5.

- The **Send Report** button in the crash reporter is no longer a default button, so there's no longer confusion about entering returns in the comment field.

- No longer prints fragments of spam messages to the console when it gets confused.

- Replaced the copy of the manual outside the app with a read-me.

2.1.2—January 26, 2004

- SpamSieve can now move Apple Mail POP messages to the **Spam** folder. Thus, it now fully supports Apple Mail on Jaguar and Panther.

- **Honor Habeas headers** is now off by default.

- Fixed regression where blocklist and whitelist rules got deselected after editing their text.

- When loading addresses from Entourage, SpamSieve now picks up addresses that are not associated with any contact (that is, they appear only in a group).

- The default date shown in the **Statistics** window is now the date that SpamSieve was first launched, rather than September 2002.

- The Apple Mail `Add Good` script is better at finding the proper inbox when moving false positives out of the **Spam** folder.

- The Apple Mail `Mark If Spam` script can mark the spam messages as read.

- The **Purchase** window now makes it more clear when a serial number has been accepted.
- In the **Statistics** window, **Set**... is now **Set Date**... and **Copy** is now **Copy Stats**.
- Fixed crash that could happen when processing messages in Japanese encodings.
- Added Japanese localization.

2.1.1—January 8, 2004

- Much faster at processing messages when there are many blocklist and whitelist rules. Also improved the speed of loading, deleting, and sorting rules.
- Improved accuracy tracking with the Panther version of Apple Mail; previously, SpamSieve couldn't always tell when it was being corrected.
- Catches more spam because it knows about more spammer obfuscation tricks and also which headers it should ignore.
- Fixed bug (introduced in 2.0) where the Bayesian engine didn't work if Mac OS X's default language was set to Japanese.
- The SpamSieve Eudora Plug-In is better at launching the SpamSieve application if it is not already running.
- Loading Entourage addresses now adds to the addresses that were previously loaded, rather than replacing them. This makes it possible for Entourage users who have more than one Entourage identity to give SpamSieve the addresses from all their address books (by loading once for each identity). Hold down Option when clicking Load to get the old behavior of replacing the previously loaded addresses.
- The sound pop-up menu in the **Preferences** window now immediately notices when new sounds are installed; previously, it would only check when updating the rest of the preferences window.
- You can now add a rule without a the **Blocklist** or **Whitelist** window being frontmost. SpamSieve will ask which type of rule to add.
- Regex rules can now start with an options modifier such as `(?-i)`.
- Copying rules to the clipboard now just copies the text to match (typically an e-mail address), not all the columns. To get all the columns, you can print to PDF.
- The Entourage `Add Good` script now finds localized inboxes, rather than creating a folder called **Inbox**.
- The Entourage `Add Spam` script can now remove spam messages from the server.
- **The Statistics** window now shows percentages instead of ratios.
- SpamSieve will now quit at launch if another copy of the application is already running.
- Re-targeted broken Habeas URL.
- Added the following menu commands: **Close All Windows**, **Minimize All Windows**, and **Zoom**.

2.1—December 9, 2003

- Added support for Apple Mail POP accounts. POP messages can be marked as junk and colored, but (due to limitations in the present version of Apple Mail) they cannot be moved to another mailbox.

- Added a **Training Tip** window that gives advice on how to improve SpamSieve's accuracy, based on the current state of the corpus and preferences.

- Rules in the whitelist and blocklist are no longer limited to just matching sender addresses. They can now match a variety of message fields (To, CC, Subject, etc.), as well as the message body. In addition to exact matches, rules now support the following match styles: contains, starts with, ends with (useful for matching domains), and Perl-compatible regular expressions. You can now edit rules and add new rules manually (as opposed to automatically, as a result of training SpamSieve with a message).

- When trained with a good message from a mailing list, SpamSieve will automatically create a whitelist rule based on a mailing list header, if present.

- SpamSieve can now read in the Entourage address book and use it as a whitelist. Thus, the Entourage rule can now give SpamSieve all the messages, not just the ones that were from unknown senders. This means that SpamSieve can now accurately notify the user when non-spam messages are received. Also, the statistics it keeps will be more complete.

- Improved the accuracy of the Bayesian classifier when the corpus is unbalanced.

- Made a variety of low-level changes to improve SpamSieve's accuracy, for instance: adjusted the list of headers that are analyzed and how words are tokenized.

- The Apple Mail `Add Spam` script now has an option to control whether the messages are moved to the **Spam** folder.

- The Entourage `Add Good` script now moves messages to the inbox if they're located in the **Spam** folder.

- Mailsmith users can now auto-train using only spam or good messages by turning off training in Mailsmith and turning on one of the auto-train checkboxes in SpamSieve.

- Improved the importing of mbox files that do not have blank lines between the messages, such as some Eudora mailboxes. Fixed a bug where the the mbox parser could crash if a message had length zero. Also, SpamSieve now shows a progress bar while counting the number of messages that will be imported.

- Improved the corpus and rule list displays. You can now enter and leave editing mode by typing Return. Type-ahead works better; for instance, if you type "g" and there are no rows that start with "g," it will look for one that starts with "f." When you delete a word or rule, you can cancel out of the confirmation sheet by typing Escape. To avoid the confirmation sheet entirely, you can delete using Command-Delete instead of Delete. When a word or rule is deleted, SpamSieve selects a nearby rule so that you don't lose your place. When deleting many words at once, SpamSieve no longer shows a progress window for deletions that will not take very long.

- Entering the name and serial number to personalize SpamSieve is now more foolproof: SpamSieve strips leading and trailing whitespace, and it detects when you enter a coupon

code in the serial number field. Fixed regression where SpamSieve rejected names containing non-ASCII characters. In addition, there's a new button for quickly redeeming coupons.

- Updated to the latest eSellerate SDK so that purchasing SpamSieve from within the application is faster.
- SpamSieve now requires Mac OS X 10.2.6 or later.
- Fixed bug where dates entered in the **Statistics** window were sometimes parsed in GMT instead of the local time zone, thus causing the date to be off by a few hours.
- Improved the reliability and user interface of the crash reporter.
- No longer crashes when parsing certain non-RFC822-compliant Eudora messages.

2.0.2—October 1, 2003

- Now works with Apple Mail (IMAP and .Mac only, not POP).
- The message count in the Dock icon now resets when an e-mail client becomes active (rather than just when SpamSieve became active). You can also control the size and position of the number in the Dock icon.
- Much faster at deleting lots of rules at once.
- Replaced the message store database with custom code that's faster and more reliable.
- Improved accuracy for HTML messages containing links.
- Importing mbox files is faster.
- Fixed bug where you couldn't use Web registration after the demo period had expired.
- The log records which addresses matched the whitelist or blocklist.
- The log records corpus imports.
- Auto-training is faster.
- The Entourage Add Spam script can close the frontmost window if it's spam.
- Fixed bug where the date in the **Statistics** window could get cut off if you changed it to use a more verbose format.
- Worked around OS bug that caused dates like "01.09.2003" to be interpreted as January 9 in German-style locales.
- Added **Copy** button to the **Statistics** window.
- Fixed problem updating certain history databases from 1.3.1.
- More resilient to minor corpus file corruption.
- Fixed crash that could happen with improperly formed multi-part messages.
- Shows the number of blocklist or whitelist rules in the title bar.
- The whitelist now contains some c-command.com addresses by default.
- Fixed crash when opening the **Statistics** window while adding messages.
- The **Statistics** window shows ratios, where applicable.
- Assorted minor performance improvements.

- The modification dates of the AppleScripts are now the actual modification dates, not the date the distribution was built.

2.0.1—September 17, 2003

- Replaced the database engine that was being used to store the corpus with some custom code. This should be much faster and more reliable.

- Loading and saving the rules is faster, due to a better file format.

- The rules and corpus message counts are now saved to disk during idle time rather than when quitting. This should prevent data loss in the event that SpamSieve doesn't quit normally.

- The whitelist and blocklist are more memory-efficient.

- Plugged memory leak in EDMessage.

- Fixed crash involving certain really long header lines.

- Fixed bug where the **Whitelist** and **Blocklist** windows weren't always up to date.

- Table views are smarter about not scrolling unnecessarily to maintain their selections.

- The **Whitelist** and **Blocklist** windows now secondary sort by sender.

- Changes to the preferences are saved to disk immediately.

- Fixed bug where tables saved their sorted columns but didn't restore them.

- When SpamSieve gets a fatal error, it now quits like it says it will.

2.0—September 10, 2003

- SpamSieve now extracts *a lot* more information from each message. This makes it much more accurate and also makes it learn faster.

- Now integrates with Eudora 6 (Sponsored or Paid) via a plug-in. It can now process every incoming Eudora message and can be trained using the **Junk** and **Not Junk** commands in Eudora's **Message** menu.

- SpamSieve now has a blocklist and a whitelist. These are automatically maintained based on the senders of messages that SpamSieve is trained with. The blocklist makes sure that all messages from known spammers are caught and speeds processing for these messages. The whitelist lets you be sure that certain messages will never be marked as spam; this was possible before, but now you don't have to clutter your address book with addresses from online retailers, etc.

- You can now control how conservative or aggressive SpamSieve is at catching spam.

- SpamSieve can now play a sound or bounce its Dock icon after a batch of non-spam messages has arrived. This is meant to replace your e-mail client's new mail notification, which you don't want going off if all the new messages are spam.

- Shows the number of new good messages in the Dock icon.

- Now parses HTML so that it can better extract relevant information from HTML messages, and also handle various HTML-based tricks that spammers use to fool filters.

- New method of calculating word probabilities makes SpamSieve better at discerning which words in the message are important.

- Includes a corpus of seed spam, to jump-start spam recognition for users who do not have many saved spam messages.

- The corpus is now stored in databases rather than in a property list. This makes it launch faster and use much less memory, as the corpus doesn't have to be all in RAM at the same time.

- The statistics file format (for History.db) has changed in order to enable performance improvements and more statistical displays in future versions.

- Handles more types of plain text obfuscations, and is much faster at undoing them.

- Added option for the address book whitelist to only use other people's addresses, so that spam messages from your own address don't match the whitelist.

- Can mark all messages with Habeas headers as good.

- Can mark all messages with some variant of "ADV" at the start of the subject as spam.

- Can mark all base64-encoded HTML messages as spam.

- New probability combiner increases accuracy.

- Uses stop words to speed processing and reduce false negatives.

- When filtering a message, considers the number of occurrences of the words, not just which words are present.

- Can import messages from mbox files.

- Can import the corpus from and export it to an XML property list (the same format used by 1.x).

- SpamSieve can now check for updated versions of itself.

- Added crash reporter.

- Added Dock menu containing frequently used commands.

- The entries in the log are more detailed.

- The corpus now stores the date at which each word was last accessed.

- Fixed bug where storing statistics would fail on systems that didn't know about GMT.

- Fixed bug where SpamSieve could throw away long runs of HTML thinking they were attachments.

- Added button for opening the Mac OS X Address Book from inside SpamSieve.

- The **Statistics** window now has a contextual menu item for copying the displayed information.

- SpamSieve no longer wastes cycles updating the **Statistics** window after it's been closed.

- The **Statistics** window is smarter about updating only the portions that could have changed.

- No longer shows Good Words and Spam Words stats.

- Logging has less overhead.

- Updates the history asynchronously, resulting in faster message processing.
- Checks for mistakes in a background thread.
- False negatives are now written to disk in a background thread.
- Re-arranged the **Corpus** window.
- Pruning the corpus now works by access date rather than by word counts. Of course, you can manually prune the old way by sorting the **Corpus** window by **Total**.
- Updated to SQLite 2.8.6 and tuned it for speed.
- Updated to PCRE 4.3.
- Updated to eSellerate 3.5, which should fix crashes some people saw after registering on 10.2.6.
- Now looks at headers of subparts of messages from Mailsmith.
- Time-consuming operations now either have a progress bar or a progress spinner.
- Better at extracting malformed e-mail addresses from headers.
- Copying rows from the **Corpus** window to the clipboard now uses the order of the columns in the window rather than the default column order.
- Fixed regression where the Entourage scripts no longer created the **Spam** folder if it didn't exist.
- Fixed potential crash with regex replacements at the end of a string.
- History.db and the corpus can now be aliases.
- Automatically trims carriage returns and other illegal characters when you paste in your name and serial number.
- Now saves the name and serial number to disk as soon as they're entered.
- The **Spam** folder in Entourage no longer has to be top-level.
- Entourage can mark good messages as unread.
- Type-selecting in table views is quicker.
- No longer nags constantly when unregistered.
- Fixed bug where it could *look* as though SpamSieve had hung if it started up in the background with an empty corpus.

1.3.1—June 18, 2003

- Added direct integration with Mailsmith 2.0 and later. Enabling SpamSieve is as easy as clicking a checkbox. You can train SpamSieve directly from Mailsmith's Message menu. Bare Bones Software has seamlessly integrated it with Mailsmith's powerful filtering system, and Mailsmith knows not to bounce its Dock icon after receiving a batch of messages that are all spam.
- Fixed crashing bug triggered by incorrectly encoded headers.
- Regex substitutions are faster and much more memory efficient.
- When adding spam messages to the corpus, the default is now for SpamSieve to move them to the **Spam** folder.

- The PowerMail **Move If Spam** script now changes the color of spam messages.
- The Emailer scripts now pass text and HTML attachments on to SpamSieve for analysis.
- Added instructions for using the Entourage and PowerMail address books as whitelists.
- Compacted the ED frameworks to reduce application size and memory use.
- Disabled SQLite's file locking so that SpamSieve's data folder can now be located on an AppleShare volume.
- Caches the Address Book to speed whitelist lookups 100 fold.
- The statistics database is faster due to an updated version of SQLite.
- Fixed bad pointer in header extractor that caused unnecessary fallbacks to the secondary parser (reducing accuracy).
- Added experimental support for moving Entourage messages on IMAP accounts to the (local) **Spam** folder. This can be enabled by editing the scripts with Script Editor.
- For clarity, the names of AppleScripts that ask SpamSieve to predict the category of a message now contain the word "if."
- Added lots of minor clarifications to the documentation.

1.3—February 11, 2003

- More resilient to spammers' tricks for obfuscating words.
- Can use e-mail addresses in the system Address Book as a whitelist. Messages sent from those addresses will never be marked as spam.
- Greatly reduced overall memory usage as well as launch and quit times.
- Can save false negatives to disk for later reporting to SpamSieve's developer.
- You can edit the spam and good counts associated with a word, remove selected words from the corpus, and reset the corpus entirely.
- Type-ahead navigation in the **Corpus** window. Type the first few letters of a word or number to select it (and scroll to it).
- You can hide statistics from before a set date, to better see the current accuracy and spam reception rate.
- Improvements to the **Corpus** window: Shows all words rather than only those considered statistically significant. Re-sorting by numeric columns is twice as fast. You can copy the selected rows to the clipboard or drag them to another application. The selection is preserved when you change the sort column, you can sort in descending order, and the sorted column is remembered between launches. The Home and End keys work.
- The **Prune Corpus** command now tells you how many words it would remove and asks for confirmation.
- The statistics tracking is smarter about handling duplicate messages.
- The statistics have tooltips explaining what they mean, and you can copy all of the statistics to the clipboard at once.
- Improved accuracy tracking of PowerMail and Emailer messages.

- Eudora Integration: Can mark spam messages as read and/or mark them for removal from the server.

- Expanded the AppleScript dictionary, to enable better integration with mail and news clients.

- Entourage Integration: Creates Junk category if there isn't one, and can mark spam messages as read.

- Mailsmith Integration: The adding scripts now set the appropriate message properties.

- Better parsing of messages with illegal characters in the headers.

- SpamSieve's Info.plist file contains an `LSUIElement` entry. Change the `0` to a `1` to hide the application's Dock icon. (You'll need to change it back to access the preferences.)

- The message count display has moved from the **Corpus** window to the **Statistics** window.

- Better error message when the corpus couldn't be saved.

- Added tooltips to preferences.

- The registration window gives better feedback when you personalize.

- Better recovery from errors in the corpus file.

- The secondary parser is better at handling DOS linebreaks.

1.2.2—November 20, 2002

- Fixed bug in the PowerMail **Add Good** script.

- Added uninstaller for Eudora users.

- Better handling of errors while adding messages to the corpus.

- Removed bloat from the Entourage **Mark Spam** script.

- The application icon now has an alpha channel, so it doesn't appear with a white halo when viewed on a colored background.

- Minor changes to the manual.

1.2.1—November 18, 2002

- Modified Info.plist to work around a bug in Mac OS X 10.1 that could cause the Finder to crash when launching SpamSieve.

1.2—November 18, 2002

- Added support for Emailer 2.0v3 and Eudora (5.2 and later).

- Decodes base64 and quoted-printable text parts, thus finding words that spammers try to hide from anti-spam software.

- Decodes subjects that use different character sets (e.g. big5).

- Adds special tokens for MIME entities such as part boundaries and uninterpretable message parts.

- Keeps track of the messages added to the corpus, and can optionally prevent you from adding the same message more than once (biasing the counts). Thus, you no longer have to remember which messages you've already added.

- You can now "undo" adds to the corpus, e.g. if you added a message as good when you meant to add it as spam.

- Can now add messages to the corpus as they are filtered, so after the initial training you only have to add messages when SpamSieve makes a mistake.

- When filtering a message, SpamSieve can optionally check whether the message is in the corpus. If it is, SpamSieve looks up the answer rather than trying to predict. One use of this feature is that if SpamSieve makes a mistake, you can **Add Spam** and then **Label/Move If Spam** and be sure that the message will be labeled/moved.

- Keeps a log of additions to the corpus, filtering results, and errors.

- Mailsmith: If SpamSieve thinks a message is spam, it sets the **deleted** property of the message to true; otherwise it sets the **flagged** property of the message to true. Therefore, if SpamSieve has classified the message then exactly one of the properties will be true, and if it hasn't they'll both be false. (Normally, neither of these message properties is used by Mailsmith itself.)

- Entourage and PowerMail: If you tell SpamSieve to move spam messages to a spam folder and the spam folder doesn't exist, the script will create the spam folder for you.

- When you add spam messages to the corpus, can optionally move them to a **Spam** folder.

- Added status indicators in the Dock icon (like Norton DiskLight).

- The spam probability of unknown words is now 0.4 instead of 0.2.

- The **Corpus** window uses less memory and sorts much faster.

- Accuracy tracking is faster and uses less memory and disk space.

- Fixed bug where accuracy tracking didn't work for some Mailsmith messages with multiple parts.

- Improved the manual's instructions for e-mail client integration.

- Compiled with GCC 3 for greater speed.

- Uses the latest version of the eSellerate SDK, which eliminates a crash at startup under certain circumstances.

- No longer shows the "Upgrading From 1.0" message when starting with a blank corpus.

1.1—September 19, 2002

- E-Mail Client Integration
  - Added support for PowerMail.
  - Added instructions and an AppleScript for making Mailsmith download and filter mail faster.
  - Added an AppleScript for Entourage that moves spam into a Junk folder.
- Performance

- Launches about 60% faster than 1.0.
- You can now prune the corpus to remove words that are taking up memory without contributing to spam recognition. This can also dramatically decrease SpamSieve's launch time.
- Recalculating spam probabilities is about 10% faster and uses less memory.
- Quitting is faster because SpamSieve now writes corpus changes to disk during idle time.
- Saving the corpus is slightly faster.

- Displays statistics about the number of messages filtered, SpamSieve's accuracy, and the types of words in the corpus.

- SpamAssassin's X-Spam-Status headers are now treated as single words. This means that if SpamAssassin is running on your mail server, SpamSieve will learn to respect (or ignore) its judgment.

- Does a better job of ignoring e-mail attachments, thus reducing corpus bloat.

- Installs the eSellerate Engine if it's not present, thus enabling "Instant Registration" for more users.

- Asking SpamSieve to categorize a message now forces an update of all the word probabilities. Previously, the update only happened during idle time.

- Highlights the sorted column in the **Corpus** window. The columns themselves have shorter names. There's a new "Total" column. Auto-resizing of the columns works better. You can now manually resize any column, and manual resizings and reorderings are saved between launches.

- Shows fatal errors as alert panels rather than just printing them on the console.

- The Corpus.plist data file is now sorted by word. This makes it easier to examine the corpus manually, and to compare it to other users' corpora.

1.0—September 10, 2002

- First public release.