

# SpamSieve 2.9.43 Manual

C-Command Software  
c-command.com

February 21, 2021



# Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction</b>                                     | <b>7</b>  |
| 1.1      | What Is SpamSieve?                                      | 7         |
| 1.2      | Identifying Spam  | 7         |
| 1.3      | Integration   | 8         |
| 1.4      | Main Features   | 9         |
| 1.5      | Why Choose SpamSieve?                                   | 10        |
| <b>2</b> | <b>Installing and Updating</b>                          | <b>10</b> |
| 2.1      | Requirements  | 10        |
| 2.2      | Installing SpamSieve                                    | 13        |
| 2.3      | Updating From a Previous Version                        | 14        |
| 2.4      | Reinstalling a Fresh Copy                               | 15        |
| 2.5      | Uninstalling SpamSieve                                  | 15        |
| 2.6      | Security & Privacy Access                               | 17        |
| <b>3</b> | <b>Using SpamSieve</b>                                  | <b>21</b> |
| 3.1      | Setting Up Apple Mail                                   | 22        |
| 3.1.1    | Enabling and Updating the Apple Mail Plug-In            | 27        |
| 3.2      | Setting Up Airmail                                      | 29        |
| 3.3      | Setting Up GyazMail                                     | 30        |
| 3.4      | Setting Up MailMate                                     | 33        |
| 3.5      | Setting Up Mailsmith                                    | 34        |
| 3.6      | Setting Up Outlook                                      | 35        |
| 3.6.1    | Outlook IMAP/Exchange Account Rules                     | 37        |
| 3.6.2    | Outlook Gmail Account Rules                             | 40        |
| 3.6.3    | Outlook POP Account Rules                               | 42        |
| 3.7      | Setting Up Postbox                                      | 44        |
| 3.8      | Setting Up PowerMail                                    | 45        |
| 3.9      | Setting Up Gmail, iCloud, Yahoo, AOL, or Other Web Mail | 46        |
| 3.10     | Setting Up Other Mail Clients                           | 46        |
| 3.11     | Do an Initial Training                                  | 46        |
| 3.12     | Correct All Mistakes                                    | 47        |
| 3.13     | SpamSieve and Multiple Macs                             | 49        |
| 3.14     | iPhone Spam Filtering                                   | 51        |
| 3.14.1   | Converting Your Apple Mail Setup to IMAP                | 53        |
| 3.14.2   | Recommended Mail Hosts                                  | 53        |
| <b>4</b> | <b>Customization</b>                                    | <b>54</b> |
| 4.1      | Rule Ordering   | 54        |
| 4.2      | Whitelisting Previous Recipients                        | 54        |
| 4.3      | Automatically Deleting Old Spam Messages                | 55        |
| 4.4      | Setting Up a Spam Filtering Drone                       | 57        |
| 4.4.1    | Setting Up an Apple Mail Drone                          | 58        |
| 4.4.2    | Setting Up a MailMate Drone                             | 60        |
| 4.4.3    | Setting Up an Outlook Drone                             | 60        |
| 4.5      | Customizing Using AppleScript                           | 61        |
| 4.6      | Apple Mail Customization                                | 61        |
| 4.6.1    | Faster Apple Mail Training                              | 62        |
| 4.6.2    | Change Settings (Apple Mail)                            | 64        |
| 4.6.3    | Apple Mail Keyboard Shortcuts                           | 64        |

|          |   |           |
|----------|---|-----------|
| 4.6.4    | Spam Message Colors in Apple Mail                     | 65        |
| 4.6.5    | Changing the Name of the Spam Mailbox                 | 68        |
| 4.6.6    | Using a Spam Mailbox on the Server                    | 69        |
| 4.6.7    | Marking Incoming Spam Messages                        | 70        |
| 4.6.8    | Separate Spam Mailboxes for Each Account              | 70        |
| 4.6.9    | Only Filtering Certain Accounts                       | 71        |
| 4.6.10   | Redirecting Good Messages to Another Account          | 72        |
| 4.6.11   | Consolidating Spam From Multiple Filters              | 72        |
| 4.6.12   | Filtering Spam During Power Nap                       | 74        |
| 4.6.13   | Keeping Spam Messages Out of Gmail's Archive          | 74        |
| 4.6.14   | Hiding Special Gmail Mailboxes From IMAP              | 75        |
| 4.6.15   | Apple Mail Script Rule                                | 75        |
| 4.6.16   | Processing Messages Before SpamSieve                  | 76        |
| 4.7      | Outlook Customization                                 | 78        |
| 4.7.1    | Change Settings (Outlook)                             | 78        |
| 4.7.2    | Duplicate Outlook Calendar Invitations                | 78        |
| 4.7.3    | Outlook Keyboard Shortcuts                            | 78        |
| 4.7.4    | Filtering Other Outlook Folders                       | 79        |
| 4.7.5    | Spam Message Categories (Outlook)                     | 79        |
| 4.7.6    | Separate Spam Folders for Each Account (Outlook 2011) | 80        |
| 4.8      | Backing Up Messages                                   | 80        |
| <b>5</b> | <b>Menus</b>  | <b>81</b> |
| 5.1      | The SpamSieve Menu                                    | 81        |
| 5.1.1    | About SpamSieve                                       | 82        |
| 5.1.2    | Software Update...                                    | 82        |
| 5.1.3    | Purchase...   | 83        |
| 5.1.4    | Mac App Store   | 84        |
| 5.1.5    | Install Apple Mail Plug-In                            | 84        |
| 5.1.6    | Install Entourage Scripts                             | 84        |
| 5.1.7    | Install Outlook Scripts                               | 84        |
| 5.1.8    | Show Other Scripts                                    | 85        |
| 5.1.9    | Update Address Book "Me" Card                         | 85        |
| 5.1.10   | Uninstall Apple Mail Plug-In...                       | 85        |
| 5.2      | The File Menu   | 85        |
| 5.2.1    | Import Addresses...                                   | 85        |
| 5.2.2    | Import Corpus...                                      | 86        |
| 5.2.3    | Export Corpus...                                      | 86        |
| 5.3      | The Filter Menu                                       | 86        |
| 5.3.1    | Show Corpus   | 86        |
| 5.3.2    | Reset Corpus...                                       | 88        |
| 5.3.3    | Show Statistics                                       | 88        |
| 5.3.4    | Open Log  | 91        |
| 5.3.5    | Edit Log  | 93        |
| 5.3.6    | Show Blocklist  | 93        |
| 5.3.7    | Rule Columns, Headers, and Match Styles               | 95        |
| 5.3.8    | Show Whitelist  | 98        |
| 5.3.9    | Add Rule  | 100       |

|          |  |            |
|----------|--|------------|
| <b>6</b> | <b>Preferences</b>   | <b>100</b> |
| 6.1      | Filters  | 100        |
| 6.1.1    | Check for message in corpus  | 101        |
| 6.1.2    | Use macOS Contacts   | 102        |
| 6.1.3    | Exclude my addresses   | 102        |
| 6.1.4    | Use Entourage/Outlook address book   | 103        |
| 6.1.5    | Use SpamSieve whitelist  | 104        |
| 6.1.6    | Use SpamSieve blocklist  | 104        |
| 6.1.7    | Use Habeas Safelist  | 104        |
| 6.1.8    | “ADV” messages are spam  | 105        |
| 6.1.9    | Encoded HTML mail is spam  | 105        |
| 6.1.10   | Use Bayesian classifier  | 105        |
| 6.2      | Notification   | 105        |
| 6.2.1    | Play sound   | 106        |
| 6.2.2    | Bounce Dock icon   | 107        |
| 6.2.3    | Keep bouncing  | 107        |
| 6.2.4    | Show number of new good messages in Dock                                     | 107        |
| 6.2.5    | Flash PowerMate  | 107        |
| 6.2.6    | A spam message is uncertain if   | 107        |
| 6.2.7    | Use Growl global notification system   | 108        |
| 6.2.8    | Include message bodies   | 109        |
| 6.3      | Training   | 110        |
| 6.3.1    | Allow duplicates in corpus   | 110        |
| 6.3.2    | Auto-train with incoming mail  | 111        |
| 6.3.3    | Train SpamSieve whitelist  | 111        |
| 6.3.4    | Train SpamSieve blocklist  | 112        |
| 6.3.5    | Train Bayesian classifier  | 112        |
| 6.4      | Advanced   | 113        |
| 6.4.1    | Spam-catching Strategy   | 113        |
| 6.4.2    | Save false negatives to disk   | 114        |
| 6.4.3    | Use photo-realistic Dock icon  | 114        |
| 6.4.4    | Quit when mail client quits  | 114        |
| 6.5      | Esoteric Preferences   | 114        |
| <b>7</b> | <b>Frequently Asked Questions (FAQ)</b>                                      | <b>116</b> |
| 7.1      | Why is SpamSieve not catching my spam?                                       | 116        |
| 7.1.1    | Checking the Apple Mail Setup  | 117        |
| 7.1.2    | If the Apple Mail Plug-In Doesn’t Appear in the List or Doesn’t Stay Enabled | 118        |
| 7.1.3    | Resetting Mail’s Private Plug-Ins Folder                                     | 119        |
| 7.1.4    | If SpamSieve Tells You the Apple Mail Plug-In Isn’t Loading, But It Is       | 121        |
| 7.1.5    | If Apple Mail Doesn’t Check for New Messages Automatically                   | 121        |
| 7.1.6    | If Apple Mail Is Running Slowly  | 121        |
| 7.1.7    | Duplicate Apple Mail Accounts  | 122        |
| 7.1.8    | Checking the Airmail Setup   | 122        |
| 7.1.9    | Checking the Entourage Setup   | 123        |
| 7.1.10   | Checking the GyazMail Setup  | 124        |
| 7.1.11   | Checking the MailMate Setup  | 125        |
| 7.1.12   | Checking the Mailsmith Setup   | 125        |
| 7.1.13   | Checking the Outlook 2011 Setup  | 126        |
| 7.1.14   | Checking the Outlook Setup   | 127        |
| 7.1.15   | Checking the Postbox Setup   | 128        |
| 7.1.16   | Checking the PowerMail Setup   | 128        |

|         |  |     |
|---------|--|-----|
| 7.1.17  | Checking the Training  | 129 |
| 7.1.18  | How do I make SpamSieve catch spams sent from my own address?                                | 129 |
| 7.2     | What information should I include when I report a problem?                                   | 130 |
| 7.2.1   | Sending in an Error Report   | 131 |
| 7.2.2   | Sending in the SpamSieve Log File  | 133 |
| 7.2.3   | Sending in Screenshots   | 134 |
| 7.2.4   | Sending in False Negative Files  | 134 |
| 7.2.5   | Sending in a “Sample” Report   | 134 |
| 7.2.6   | Sending in Crash Log Files   | 135 |
| 7.2.7   | Sending in Apple Mail Rules  | 135 |
| 7.3     | Why is every message going to the Spam mailbox?  | 137 |
| 7.4     | Why do good messages keep going to the Junk or Spam mailbox?                                 | 138 |
| 7.5     | Can I delete spam messages that are in the spam folder?                                      | 138 |
| 7.6     | How should I configure the junk filter on my mail server?                                    | 139 |
| 7.6.1   | Turning Off the AOL Spam Filter  | 140 |
| 7.6.2   | Turning Off the Fastmail Spam Filter   | 140 |
| 7.6.3   | Turning Off the Gmail Spam Filter  | 141 |
| 7.6.4   | Turning Off the GoDaddy Spam Filter  | 144 |
| 7.6.5   | Turning Off the Hover Spam Filter  | 144 |
| 7.6.6   | Turning Off the iCloud Spam Filter   | 144 |
| 7.6.7   | Turning Off Microsoft Spam Filters   | 144 |
| 7.6.8   | Turning Off the Yahoo Mail Spam Filter   | 146 |
| 7.6.9   | Turning Off Other Spam Filters   | 150 |
| 7.7     | Why does a message disappear or go back to the spam mailbox after I train it as good?        | 150 |
| 7.8     | Does SpamSieve protect me from viruses?  | 152 |
| 7.9     | Does SpamSieve stop Web bugs?  | 152 |
| 7.10    | Does SpamSieve bounce spam messages back to the sender?                                      | 154 |
| 7.11    | Does SpamSieve prevent me from receiving messages?   | 154 |
| 7.12    | SpamSieve Application Questions  | 156 |
| 7.12.1  | Why doesn’t my serial number work?   | 156 |
| 7.12.2  | Should I download SpamSieve from this free site?   | 156 |
| 7.12.3  | How can I hide SpamSieve’s Dock icon?  | 157 |
| 7.12.4  | How can I copy my training data to another machine?  | 157 |
| 7.12.5  | Does SpamSieve launch automatically?   | 158 |
| 7.12.6  | Can I use SpamSieve with more than one mail program at a time?                               | 159 |
| 7.12.7  | Why does SpamSieve need to access my contacts?   | 159 |
| 7.12.8  | How can I open the Library folder?   | 159 |
| 7.12.9  | What can I do if the corpus file is damaged?   | 160 |
| 7.12.10 | What can I do if the statistics database is damaged?   | 161 |
| 7.13    | Apple Mail-Specific Questions  | 161 |
| 7.13.1  | Why does the “Junk” mailbox appear in Apple Mail?  | 161 |
| 7.13.2  | Why don’t I see the SpamSieve commands in Apple Mail’s Message menu?                         | 163 |
| 7.13.3  | Why do good messages move to the wrong inbox when trained in Apple Mail?                     | 165 |
| 7.13.4  | Why do I see spam messages in my “Unread” smart mailbox in Apple Mail?                       | 166 |
| 7.13.5  | Why does the Spam mailbox in Apple Mail appear empty even though there’s a number beside it? | 166 |
| 7.13.6  | What can I do if my Spam mailbox in Apple Mail disappeared?                                  | 167 |
| 7.13.7  | Why are messages marked as spam in Apple Mail but not moved?                                 | 167 |
| 7.13.8  | Why does SpamSieve always need an update when macOS is updated?                              | 168 |
| 7.13.9  | Why do Apple Mail messages bounce back to the inbox after I train them as spam?              | 170 |
| 7.13.10 | How can I rebuild Apple Mail’s database?   | 170 |

|  |            |
|--|------------|
| 7.13.11 How can I reset Apple Mail's junk database?                  | 172        |
| 7.13.12 Can other Apple Mail plug-ins cause problems with SpamSieve? | 173        |
| 7.13.13 What can I do if Apple Mail is crashing?                     | 173        |
| <b>8 Legacy Mail Programs</b>  | <b>174</b> |
| 8.1 Setting Up Airmail 1–3   | 174        |
| 8.2 Setting Up Entourage   | 176        |
| 8.2.1 Entourage Customization  | 179        |
| 8.3 Setting Up Entourage v.X   | 181        |
| 8.4 Setting Up MailForge   | 185        |
| 8.5 Setting Up Outlook 2011  | 185        |
| 8.6 Setting Up PowerMail 4   | 190        |
| <b>9 Legal Stuff</b>   | <b>192</b> |
| <b>10 Version History</b>  | <b>195</b> |

# 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, the spam problem has gotten worse. Today’s spam is harder to detect, and there is more of it. Without the assistance of a good spam filter, you’ll waste valuable time sorting through your inbox manually.

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 junk mail, 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, Exchange, 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 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](#)<sup>1</sup> 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 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.

---

<sup>1</sup><http://www.paulgraham.com/spam.html>

## 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.
- SpamSieve works with any mail provider/host. It filters all your mail accounts. There is no extra charge for additional addresses or devices.
- SpamSieve running on your Mac can [keep the spam off your iPhone/iPad](#), and you can even train SpamSieve [from afar](#).
- Colors show [how spammy](#) each message is, so you can quickly focus on the [borderline ones](#) if you want to check SpamSieve's work.
- Integrates with the [macOS Contacts app](#) 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.
- Unlike server-based spam filtering services, your mail data stays on your own Mac, so your privacy is preserved.
- SpamSieve [supports AppleScript](#), so you can connect it to additional apps and fully integrate it into a custom workflow.

## 1.5 Why Choose SpamSieve?

Given that e-mail programs such as Apple Mail 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. Secondly, SpamSieve will give you peace of mind because it is far less likely to accidentally put good messages into the **Spam** mailbox. No more worrying about missing an important work e-mail, job lead, or message from a friend.

The same is true if your mail provider, such as Gmail, already offers a server-side junk filter. Lots of SpamSieve customers have Gmail, but they use SpamSieve in addition to or [instead of Gmail's spam filter](#) because it is missing spam messages or incorrectly catching their good messages. Even if Gmail is catching 95% or 99.0% for you, that still leaves quite a bit of room to do better (unless you don't receive much mail at all). And for good messages, SpamSieve can provide an assurance that certain addresses (e.g. from Contacts) will never go to the **Spam** mailbox.

Read what [the press](#) and [other SpamSieve users](#) 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 works with macOS 10.9 and later, as well as [pre-release versions of macOS](#). For older versions of macOS, [previous versions of SpamSieve](#) are available.

#### Supported Mac Mail Programs

SpamSieve is designed to work with the following e-mail programs that are currently under development:

- [Apple Mail](#) from macOS 10.9 and later.
- [Airmail](#)<sup>2</sup> 1.3.1 (223) and later. Versions 3.6.3 through 3.6.41 are not compatible with SpamSieve on macOS 10.14, but version 3.6.42 and later are.
- [GyazMail](#)<sup>3</sup> 1.2.0 (1.5.8 or later recommended).
- [MailMate](#)<sup>4</sup> 1.1.2 and later from Freron Software.
- [Mailsmith](#)<sup>5</sup> 2.3.1 and later from Stickshift Software. (By applying [this workaround](#) you can use SpamSieve with Mailsmith 2.1.5.)
- [Outlook](#)<sup>6</sup> from Microsoft Office 2011 (14.x) and later, including Outlook 2016 and 2019 (15.x and 16.x) from Office 365. Outlook Live and other browser-based mail are *not* supported, except via the Mac clients listed here.

---

<sup>2</sup><http://airmailapp.com>

<sup>3</sup><http://gyazsquare.com/gyazmail/>

<sup>4</sup><http://freron.com>

<sup>5</sup><http://www.mailsmith.org>

<sup>6</sup><http://www.microsoft.com/mac/outlook>

- [Postbox 2.0](#)<sup>7</sup> through 5.x from Postbox, Inc. Postbox 6 and 7 are [not currently compatible](#). Postbox Express and the (discontinued) Mac App Store version of Postbox are not compatible.
- [PowerMail](#)<sup>8</sup> 4.0 and later (6.x recommended) from CTM Development. PowerMail only supports SpamSieve with POP accounts.

## iOS Mail and Web Mail

SpamSieve does not run on iOS, but you can use it together with your Mac to filter mail on your iPhone, iPad, or iPod touch. This is described in the [iPhone Spam Filtering](#) section.

SpamSieve works with Web mail providers via Apple Mail. Please see the [Setting up Gmail, iCloud, Yahoo, AOL, or Other Web Mail](#) section.

## Supported Legacy Mac Mail Programs

SpamSieve also works with these legacy e-mail programs:

- [Entourage](#)<sup>9</sup> v.X (2001) and later (Entourage 2004 or 2008 recommended) from Microsoft.
- [MailForge](#)<sup>10</sup> 2.0.4 and later from Macsimize Software (formerly from Infinity Data Systems).

## Multiple Accounts/Addresses

SpamSieve filters all of your mail accounts. There is no extra charge for additional addresses.

## Multiple Mail Programs

You can freely switch between mail programs or even use multiple mail programs at once. SpamSieve will share its training data and statistics among them.

## Unsupported Mac Mail Programs

SpamSieve does not have direct integration with the following mail programs. You can, however, still use them with SpamSieve as described in the [Setting Up Other Mail Clients](#) section.

- [Canary Mail](#) is not sufficiently extensible for us to connect it with SpamSieve. We have offered to help the developers add support for SpamSieve, and they have expressed interest. Sending them [feedback](#) (click the blue-and-white icon at the bottom-right) will help them prioritize this feature.
- [MailPlane](#)<sup>11</sup> is not sufficiently extensible for us to connect it with SpamSieve. Please [contact](#)<sup>12</sup> the developers and tell them that you would like to use SpamSieve with it.
- [Mail Pilot](#)<sup>13</sup> is not sufficiently extensible for us to connect it with SpamSieve. We have offered to help the Mail Pilot developers add support for SpamSieve, and it's on their to-do list. Sending them feedback will help them prioritize this feature.

---

<sup>7</sup><http://www.postbox-inc.com>

<sup>8</sup><http://www.ctmdev.com/powermail/>

<sup>9</sup><http://www.microsoft.com/mac/products/entourage2008/default.mspx>

<sup>10</sup><http://macsimizesoftware.com>

<sup>11</sup><http://mailplaneapp.com>

<sup>12</sup><mailto:support@mailplaneapp.com>

<sup>13</sup><http://www.mailpilot.co>

- [Newton](#) is not sufficiently extensible for us to connect it with SpamSieve. Please [contact](#)<sup>14</sup> the developers and tell them that you would like to use SpamSieve with it.
- [Spark](#) is not sufficiently extensible for us to connect it with SpamSieve. We have offered to help the Spark developers add support for SpamSieve, and they have expressed interest. Sending them [feedback](#) will help them prioritize this feature.
- [Sparrow](#)<sup>15</sup> is not sufficiently extensible for us to connect it with SpamSieve. The Sparrow developers were interested in adding support for SpamSieve, but the product has since been acquired by Google and seems to no longer be under development.
- [Thunderbird](#). Current versions of Thunderbird have removed support for compiled plug-ins. However, SpamSieve does work with [Postbox](#)<sup>16</sup>, which is an enhanced version of Thunderbird.
- [Unibox](#) is not sufficiently extensible for us to connect it with SpamSieve. We have offered to help the Unibox developers add support for SpamSieve. Sending them feedback will help them prioritize this feature.

## Mail Program Differences

SpamSieve works roughly the same way with each mail program. This section describes features that are only available in certain mail programs.

### *Auto-Deletion*

These mail programs support [automatically deleting old Spam messages](#): Apple Mail, Entourage, Outlook (not Outlook 365), Postbox.

### *Complete Message Access*

These mail programs allow for more accurate filtering because they let SpamSieve access the entire raw source of each message, including the attachments: Apple Mail, Airmail, Entourage, GyazMail, MailMate, Mailsmith, Outlook.

### *Custom Rules*

These mail programs let you control SpamSieve through a regular rule, so that you can determine how it interacts with your other rules: Apple Mail, Entourage, GyazMail, MailMate, Mailsmith, Outlook 2011, PowerMail.

### *Drone Support*

These mail programs work with the setup described in [Setting Up a Spam Filtering Drone](#): Apple Mail, MailMate, Outlook 2011 (not Outlook 365, 2016, or 2019).

### *Refiltering Messages*

These mail programs let you manually re-apply SpamSieve to old messages: Apple Mail, Entourage, GyazMail, MailMate, Mailsmith, Outlook, Postbox, PowerMail.

### *Spam Levels*

---

<sup>14</sup><mailto:hello@newtonhq.com>

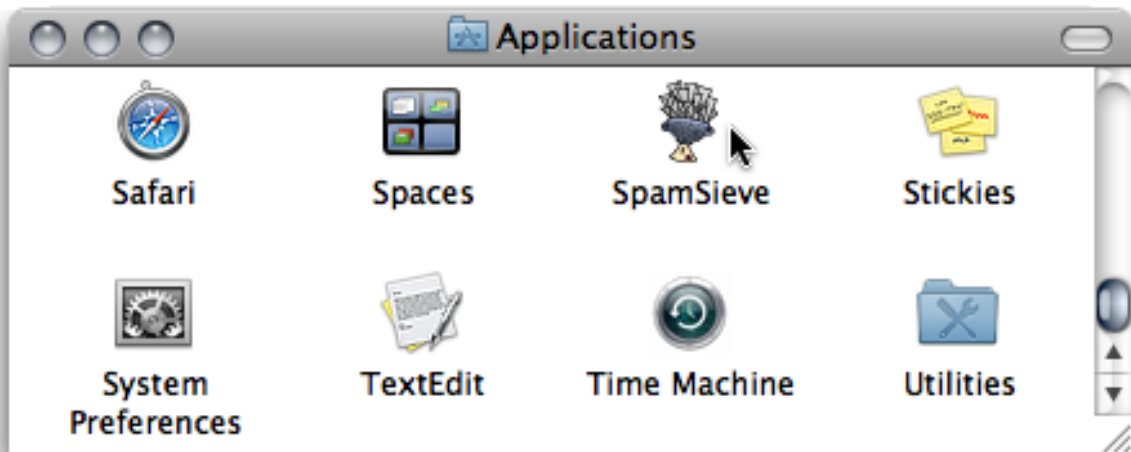
<sup>15</sup><http://sparrowmailapp.com>

<sup>16</sup><http://www.postbox-inc.com>

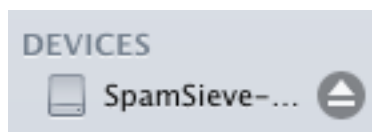
These mail programs can display spam messages in [different colors](#) or with a numeric score to indicate their level of spamminess: Apple Mail, Entourage, MailMate, Mailsmith, Outlook, PowerMail.

## 2.2 Installing SpamSieve

1. If you have not already done so, go to the [SpamSieve Web site](#) and click the **Download (Free Trial)** button. (The trial and full version of SpamSieve are the same file.) After it finishes downloading, double-click the `SpamSieve-2.9.43.dmg` file.
2. Drag the **SpamSieve** icon onto the **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.)
3. Double-click the **Applications** folder to open it.
4. Double-click the **SpamSieve** icon to launch it.



5. Eject the `SpamSieve-2.9.43` icon.



6. To enable certain SpamSieve features, please see the [Security & Privacy Access](#) section of the manual.

Next, you *must* follow the instructions in the [Using SpamSieve](#) section in order to set up your mail program to use SpamSieve.

## 2.3 Updating From a Previous Version

There are two ways to update to the latest version of SpamSieve:

### Automatic Updating

1. Launch your old version of SpamSieve.
2. Normally, SpamSieve will automatically check for updates and detect that a new version is available. If you have turned that feature off or don't want to wait for the automatic check:
  - a) Choose [Software Update...](#) from the **SpamSieve** menu. If SpamSieve's Dock icon is hidden, you can access the **Software Update...** command via the **Message ▾ SpamSieve - Open Window** command in Apple Mail or by using the [Open Window script](#).
  - b) Click the **Check Now** button.
3. Click the **Download & Install** button and follow the on-screen instructions.
4. You may be asked for an administrator password to ensure that incorrect file permissions on your Mac do not prevent the update from completing, leaving your Mac in an inconsistent state. The username and password for the automatic update are the ones for installers and logging into your Mac. They're not related to SpamSieve. If you don't know your password, you can [reset it](#) or update SpamSieve by following the "Manual Updating" instructions below.

### Manual Updating

1. Go to the [SpamSieve Web site](#) and click the **Download (Free Trial)** button.
2. Quit SpamSieve and your mail program.
3. 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.

*Note:* If you get an error saying that the file is locked or 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.
4. Launch SpamSieve and your mail program.

### macOS Updates

It's best to update SpamSieve [before](#) updating macOS. To prevent macOS from updating itself without asking you, go to the **App Store** section of **System Preferences** and make sure that **Install macOS updates** is unchecked.

### Repeated Update Prompts

If SpamSieve keeps telling you that a new version is available, even after you've updated, you may still have the old version somewhere on your Mac. There should only be one copy of SpamSieve installed, and it should be stored [directly in your Applications folder](#). If you see a window saying that you need to update

SpamSieve, you can Command-click on the SpamSieve icon in the Dock. This will reveal the location of the **SpamSieve.app** file in the Finder so that you can see where the old version is and delete it (after quitting SpamSieve).

## 2.4 Reinstalling a Fresh Copy

If your copy of SpamSieve is damaged, you may need to download and install a fresh copy.

- If you are able to launch SpamSieve, you can ask it to reinstall itself. To do this, follow the **Automatic Updating** instructions (in the [Updating From a Previous Version](#) section) but hold down the Option key when you click the **Check Now** button.
- If SpamSieve won't launch, follow the **Manual Updating** instructions in the [Updating From a Previous Version](#) section.
- If you've uninstalled SpamSieve, you can always get it back by going to the [SpamSieve Web site](#) and clicking the **Download (Free Trial)** button. After installing it, you can enter your **Serial Name** and **Serial Number** into the [Purchase...](#) window to take it out of trial mode. If you can't find your serial number, you can [look it up online](#).

## 2.5 Uninstalling SpamSieve

### Please Contact Us

If you are considering uninstalling SpamSieve because you're having trouble using it or it doesn't seem to meet your needs, please see [this page](#) or contact us at [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>17</sup>. We're happy to help get you up and running and always looking for suggestions for how to improve SpamSieve.

### Temporarily Disabling SpamSieve

To temporarily disable SpamSieve, you can just uncheck the SpamSieve rule(s) that you created in your mail program. This is a quick way to turn it off if you don't want your mail to be filtered for a while. For example, it can be helpful to turn off spam filtering while you are troubleshooting your other mail rules.

### Removing SpamSieve's Application Files

If you are using Apple Mail, first choose **Uninstall Apple Mail Plug-In...** from [the SpamSieve menu](#). (If you can't see that menu after launching SpamSieve, you may have hidden SpamSieve's Dock icon and need to [show it](#) again.)

To completely uninstall SpamSieve, drag the [SpamSieve application file](#) in your **Applications** folder to the trash.

Additionally, follow the instructions below that are specific to your mail program:

#### *Apple Mail*

If you already chose **Uninstall Apple Mail Plug-In...** from [the SpamSieve menu](#), you can skip these steps.

---

<sup>17</sup><mailto:spamsieve@c-command.com>

Or, to manually uninstall, follow these steps:

1. If you are using a single Mac, make sure that you've deleted the **SpamSieve** rule in Mail's preferences (described in [Setting Up Apple Mail](#)). If you are using multiple Macs and wish to continue using SpamSieve on one of the others, you wouldn't want the deletion to propagate through iCloud, so you should uncheck the rule rather than deleting it.
2. Quit Apple Mail.
3. Delete these files:

```
/Users/<username>/Library/Mail/Bundles/SpamSieve.mailbundle  
/Library/Mail/Bundles/SpamSieve.mailbundle  
/Users/<username>/Library/Mail/SpamSieve/  
/Users/<username>/Library/LaunchAgents/com.c-command.SpamSieve.LaunchAgent.plist  
/Users/<username>/Library/Application Scripts/com.apple.mail/Launch SpamSieve.scpt  
/Users/<username>/Library/Application Scripts/com.apple.mail/SpamSieve Move If Spam.scpt
```

See the [How can I open the Library folder?](#) section for how to get to these files. After opening the **Library** folder, drag the three items above to the trash. If you do not do this, Mail will report an error saying that it could not find SpamSieve.

As an example, to remove the first file, open the **Library** folder. Inside the **Library** folder there is a **Mail** folder. Inside of that is the **Bundles** folder. Inside of that is the **SpamSieve.mailbundle** that you should drag to the trash.

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

### *Airmail*

Uncheck the **Use SpamSieve** checkbox in the **Advanced** section of the preferences (described in [Setting Up Airmail](#)).

### *GyazMail*

Delete the **SpamSieve** rule (described in [Setting Up GyazMail](#)).

### *MailMate*

Uncheck **SpamSieve** (described in [Setting Up MailMate](#)).

### *Mailsmith*

Uncheck **Use SpamSieve** (described in [Setting Up Mailsmith](#)).

### *Outlook 365*

Delete the SpamSieve script files in the folder:

```
/Users/<username>/Library/Scripts/Applications/Microsoft Outlook
```

and the **Outlook - Filter Mailboxes.app** application if you are using it.



### *Outlook 2011*

Delete the SpamSieve script files that are located in the **Outlook Script Menu Items** folder inside **Microsoft User Data** (which is probably in your **Documents** folder).

Additional scripts are located in the folder:

```
/Users/<username>/Library/Application Support/Microsoft/Office/Outlook Script Menu Items/
```

See the [How can I open the Library folder?](#) section for how to get to this folder.

### *Postbox*

Choose **Add-ons** from Postbox's **Tools** menu. Click the **remove** button next to **SpamSieve Postbox Plug-in**.

### *PowerMail*

Go to the **Spam filter assistant** (described in [Setting Up PowerMail](#)).

## **Removing SpamSieve's Data Files**

You can optionally delete SpamSieve's data files, which are stored at:

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

See the [How can I open the Library folder?](#) section. If you delete these files, you will have to re-train SpamSieve if you reinstall it.

## **Legacy Mail Programs**

These are the files to remove for other mail programs:

### *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 choose **Junk E-mail Protection...** (or **Junk Mail Filter** in Entourage v.X) and re-enable Entourage's junk mail filter.

## **2.6 Security & Privacy Access**

On macOS 10.14 and later, you need to tell the system if you want applications to be able to control other applications or access their data. For example:

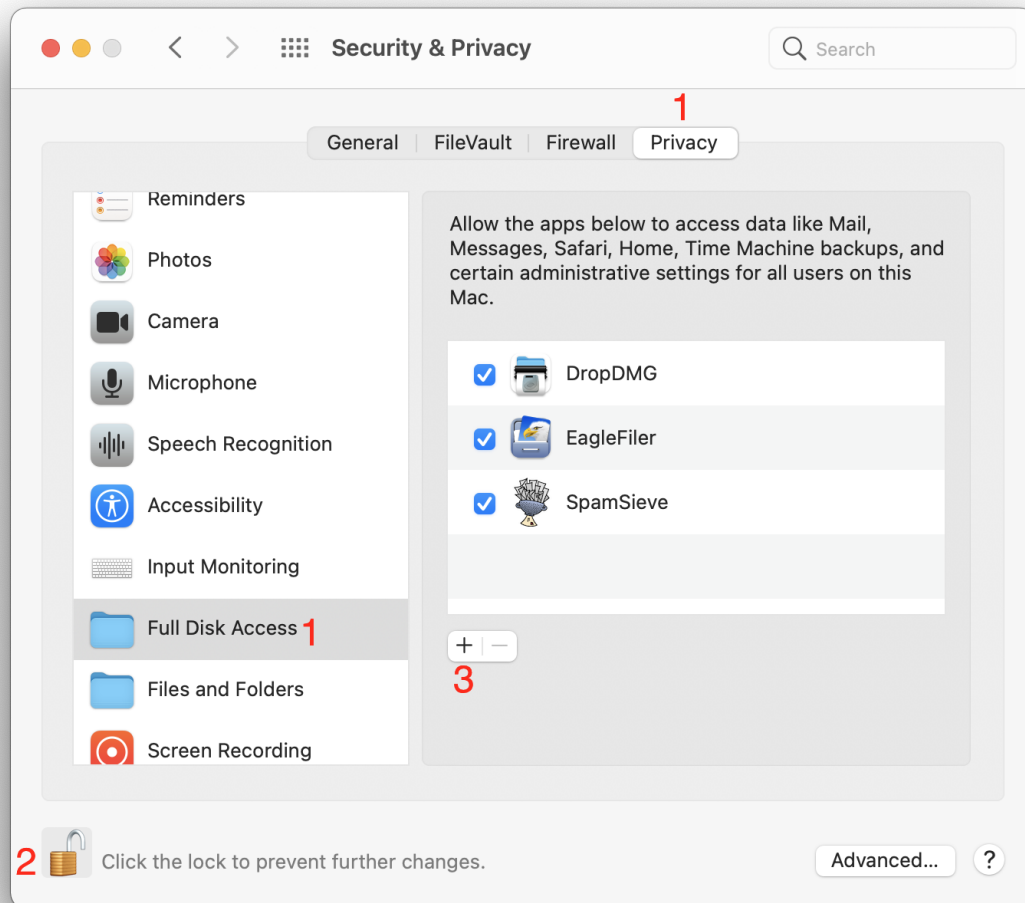
- In order to install the plug-in for Apple Mail, SpamSieve needs full disk access to copy the plug-in into Mail's folder.

- In order to train messages in Apple Mail, SpamSieve needs to be able to control Mail to ask about the selected messages.

## Granting Full Disk Access

To give SpamSieve access:

1. Go to the **Security & Privacy** pane of System Preferences and click on the **Privacy** tab. Then scroll down and click on **Full Disk Access**. (You can also [click here](#) to go directly to **Full Disk Access**.)



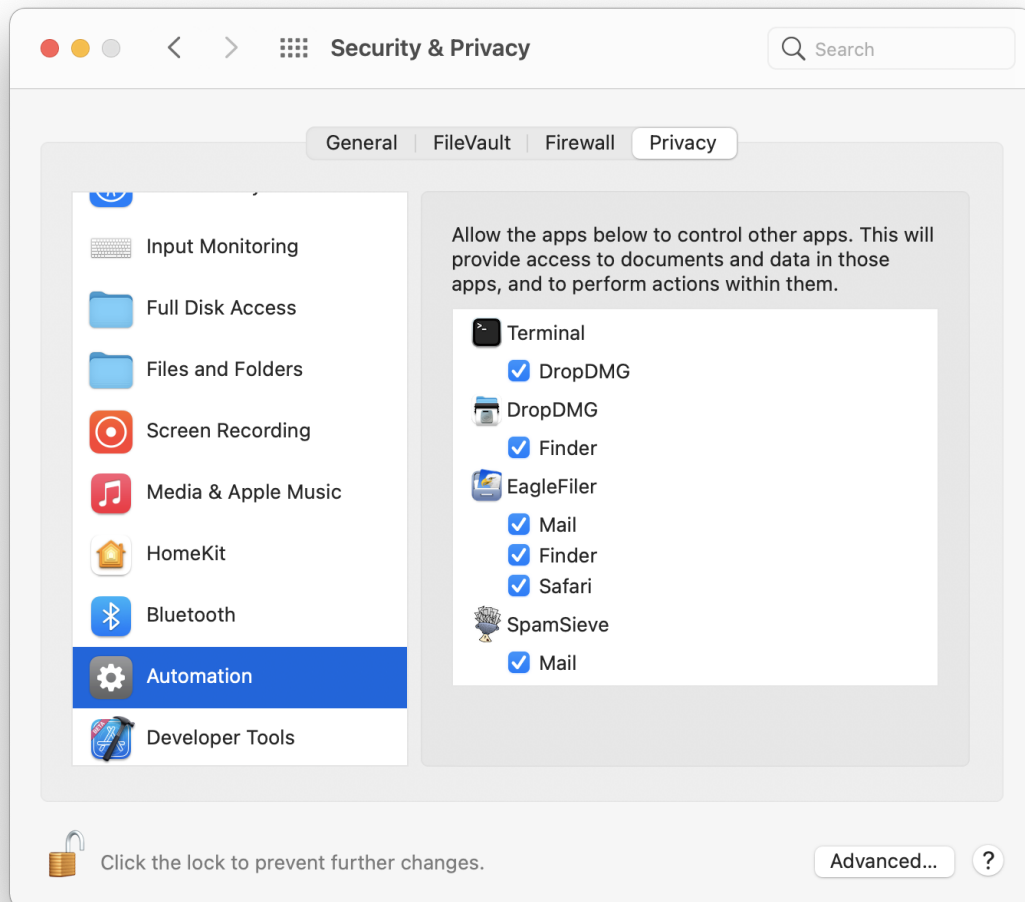
2. If the lock button in the lower left corner of the window is locked, click on it, enter your Mac's login password, and click **Unlock** so that you are allowed to make changes.
3. Click the + button and choose SpamSieve from your **Applications** folder. Click **Quit Now** if applicable. SpamSieve should now appear in the list as checked.

4. Double-click the SpamSieve icon to relaunch it.

### Granting Automation Access

macOS will automatically ask you when SpamSieve needs to be able to control an application. It will show an alert, and you should click the **OK** button.

If you accidentally click **Don't Allow** and deny SpamSieve access to control an app, macOS will remember this and may not ask you again. You can add access by going to **Security & Privacy** ▸ **Privacy** ▸ **Automation** in System Preferences ([click here](#)) and checking the box(es) under SpamSieve.



### Troubleshooting Full Disk Access

In rare cases, SpamSieve may not appear in the **Full Disk Access** list after you add it. You can enter this command in Terminal:

```
tccutil reset SystemPolicyAllFiles
```

to reset the system's database of file privileges and then try adding SpamSieve again.

## Troubleshooting Automation Access

You can enter this command in Terminal:

```
tccutil reset AppleEvents
```

to reset the system's database of Automation privileges. Then macOS will ask you again the next time SpamSieve needs access, and you can click **OK**. If it still doesn't ask you to grant access, it may help to restart your Mac or use the maintenance feature of [Onyx](#).

If that doesn't help, try [installing a fresh copy](#) of the app because macOS's security features won't work if the app file is damaged (which makes its code signature invalid).

## If macOS Doesn't Remember The Access You Granted or tccutil Fails

First, try the `tccutil reset` commands above.

Second, make sure that the application file is not damaged, e.g. by [reinstalling a fresh copy](#). Also, make sure that you are not modifying the application package, e.g. editing its `Info.plist` file to try to hide the Dock icon.

If it still doesn't work, you may need to reset the entire privacy database:

1. First, we will temporarily turn off [System Integrity Protection](#) so that we have access to delete the database. You may want to print these instructions or write them down so that you have access to them while rebooting your Mac.
2. Restart your Mac in Recovery Mode. The steps for doing this depend on [which type of processor](#) your Mac has:
  - On an [Intel-based Mac](#), click on the Apple menu and choose **Restart...** Hold down the Command and R keys so that your Mac will reboot in Recovery Mode.
  - On an [Apple Silicon-based Mac](#), click on the Apple menu and choose **Shut Down...** Press and hold the power button on your Mac until you see "Loading startup options." Click **Options**, then click **Continue**, then click **Continue** again.
3. From the **Utilities** menu, choose **Terminal**.
4. Type `csrutil disable` and press Return.
5. Click on the Apple menu and choose **Restart**. This is necessary for the SIP change to take effect.
6. Drag the file:

```
/Users/<username>/Library/Application Support/com.apple.TCC/TCC.db
```

to the trash. (See [How can I open the Library folder?](#) if you have trouble finding it.)
7. You can then repeat Steps 2–5, typing `csrutil enable` instead, in order to turn SIP back on.

If it *still* doesn't work, reinstalling macOS takes a while but always seems to fix the problem.

### Other Reasons SpamSieve Needs Automation Access

- In order to activate, deactivate, and uninstall the Apple Mail rule, SpamSieve needs to control Mail.
- In order to run the [Remote Training](#) or [Server Junk Mailbox](#) script, Mail needs to control SpamSieve.
- In order to create an “Uncertain Junk” category in Outlook and find where to install its Outlook scripts, SpamSieve needs to control Outlook.
- In order to whitelist messages from your Outlook or Entourage address books, SpamSieve needs to control those applications to ask them about your addresses.
- In order to update the e-mail addresses on your Contacts card, SpamSieve needs to control the mail programs that you have installed to ask them about your addresses.
- In order to filter messages in Outlook, SpamSieve's “Outlook - Filter Mailboxes” helper application needs to be able to control Outlook and SpamSieve.
- In order to flash a PowerMate when new messages arrive, SpamSieve needs to be able to control the PowerMate app.
- Airmail and MailMate need to control SpamSieve to send it messages to analyze.

## 3 Using SpamSieve

There are four basic steps to installing and using SpamSieve:

1. Put the SpamSieve application in your applications folder. This is described in the [Installing SpamSieve](#) section.
2. Set up your mail program to use SpamSieve to filter your mail. This is described in sections 3.1 through 3.10 (below) and in the [Legacy Mail Programs](#) section (e.g. for Microsoft Entourage and Outlook 2011). Find the section below that corresponds to the mail program that you're using.
3. Train SpamSieve with some examples of your spam and good messages, as described in the [Do an Initial Training](#) section. (This step is optional but highly recommended. You can skip it if you don't have any saved spam messages.)
4. SpamSieve will launch automatically when new mail arrives. It will examine each incoming message and move the spam messages to a separate mailbox. In order to keep SpamSieve's accuracy high, you'll need to tell it about any spam messages that you find in your inbox or good messages that you find in your spam mailbox. This is described in the [Correct All Mistakes](#) section.

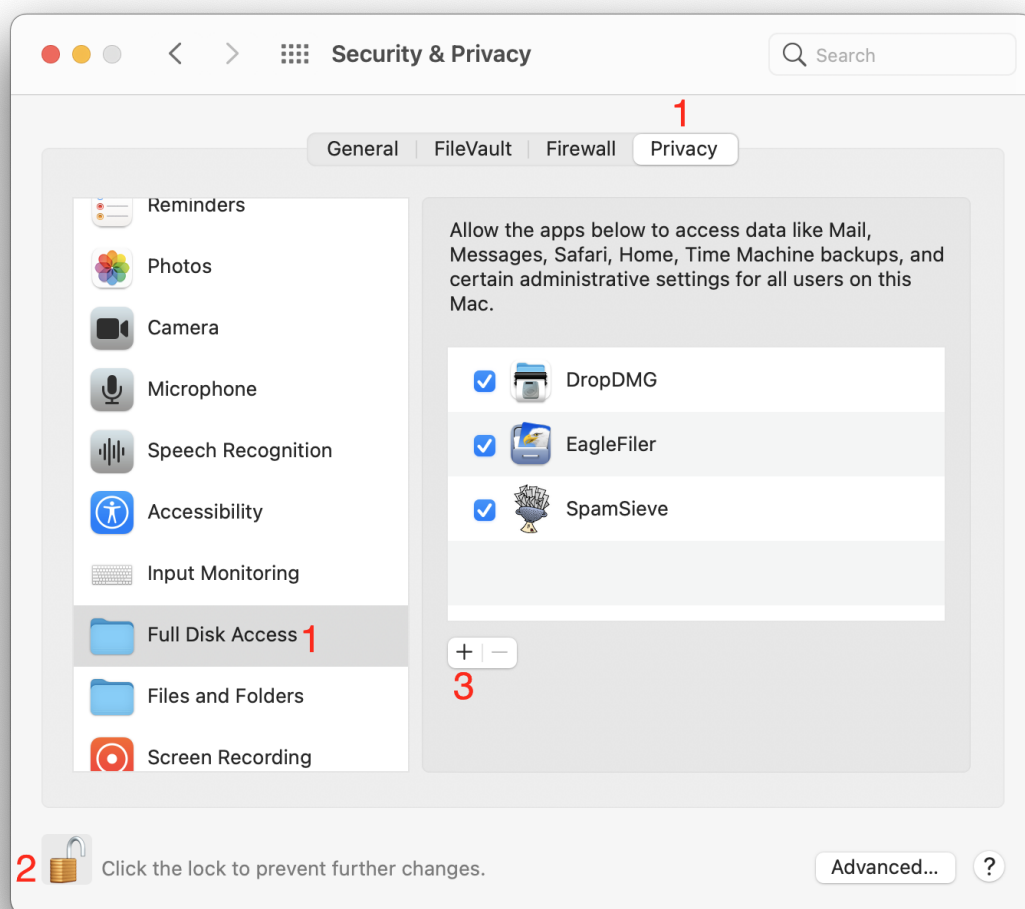
You can return to this page at any time by going to SpamSieve's **Help** menu and choosing **Setting Up and Using SpamSieve**. The **Help** menu also contains a PDF version of this manual, which is easier to search and print.

The rest of this manual contains detailed information about how SpamSieve works and how it can be customized. If you have a question, it's probably answered here. However, following the above four steps is all most users will need to do to effectively use SpamSieve.

### 3.1 Setting Up Apple Mail

In addition to these written instructions, there are a [screencast video](#) and [video review](#)<sup>18</sup> that demonstrate how to set up and train SpamSieve with Apple Mail.

1. If you are using macOS 10.14 or later, make sure that SpamSieve has full disk access by going to **System Preferences** ▸ **Security & Privacy** ▸ **Privacy**. This is described in more detail in the [Security & Privacy Access](#) section. If you are using macOS 10.13.x or earlier, you can skip this step.

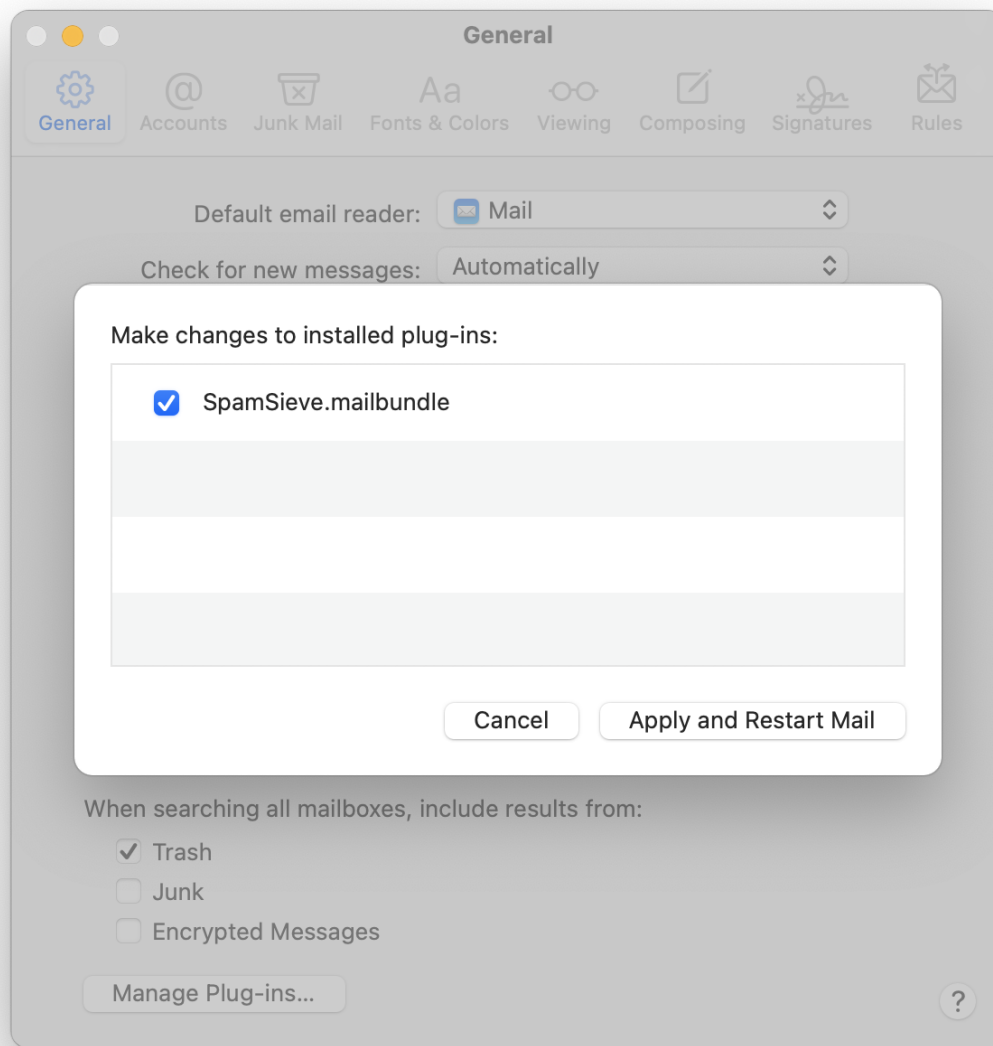


2. Quit Mail. Then double-click the SpamSieve application and choose [Install Apple Mail Plug-In](#) from the [SpamSieve](#) menu at the top-left of the screen. Now relaunch Mail.

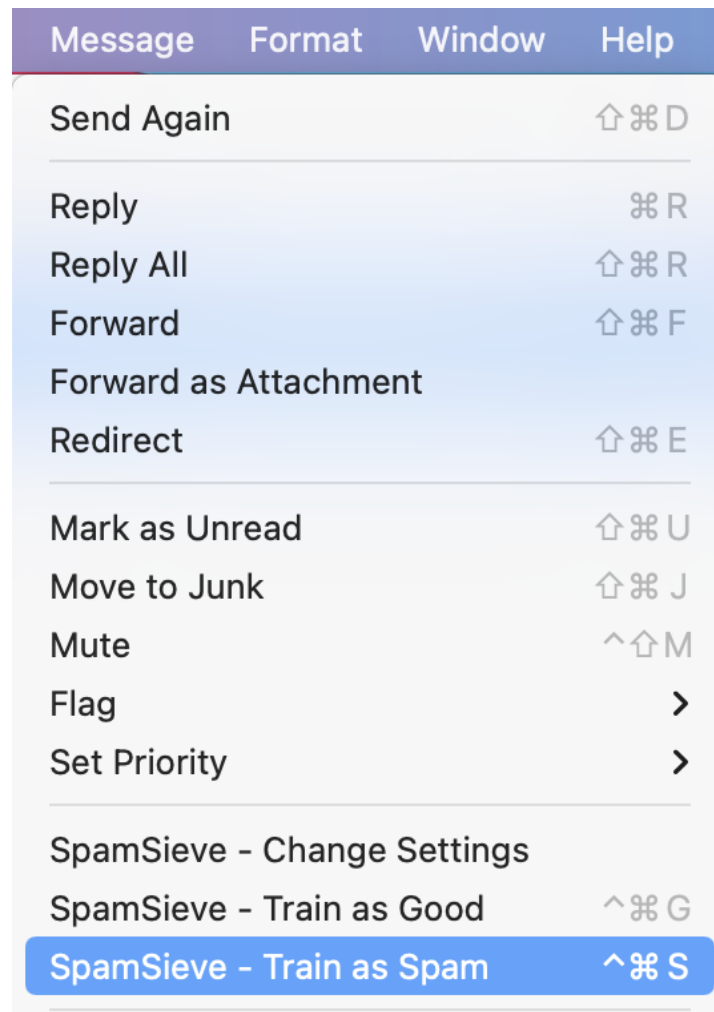
If you are using macOS 10.14 or later, you will need to click **Manage Plug-ins...** in Mail's preferences and enable **SpamSieve.mailbundle**. This is described in more detail in the [Enabling](#)

<sup>18</sup>[http://www.eurmpa.net/rev\\_id.psw.42549\\_spamsieve29.html](http://www.eurmpa.net/rev_id.psw.42549_spamsieve29.html)

and [Updating the Apple Mail Plug-In](#) section. If you are using macOS 10.13.x or earlier, you don't have to enable the plug-in.



You should now see the **SpamSieve - Change Settings**, **SpamSieve - Train as Good**, and **SpamSieve - Train as Spam** items in Mail's **Message** menu:



If you do not see these commands, please see the [Why don't I see the SpamSieve commands in Apple Mail's Message menu?](#) section.

3. Choose **New Mailbox...** (or **New...**) from 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**.

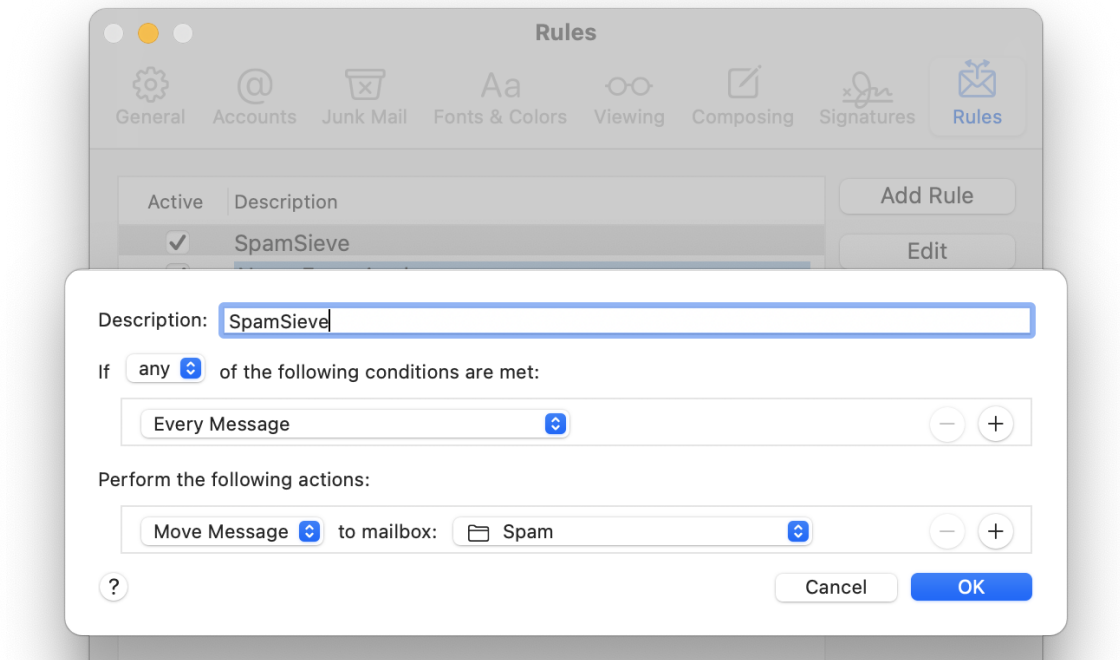
*Note:* See the [Using a Spam Mailbox on the Server](#) section if you prefer to have your spam accessible from all your devices or if you find that Mail is [leaving marked spam messages in the inbox](#). If you are using Gmail, see the [Keeping Spam Messages Out of Gmail's Archive](#) section.

4. Choose **Preferences...** from the **Mail** menu and click the **Rules** button in the toolbar. Click the **Add Rule** button. Change the description to **SpamSieve**.

*Note:* The description of the rule *must* start with **SpamSieve**, but you can add additional text after that, if you want, so long as you don't use square brackets, which SpamSieve uses those for [color rules](#).

Change the **From** (or **Any Recipient**, prior to macOS 10.12) pop-up menu to say **Every Message**. (**Every Message** is near the bottom of the menu.) Then, next to **Move Message**, select the **Spam** mailbox that you just created. The rule should now look like:

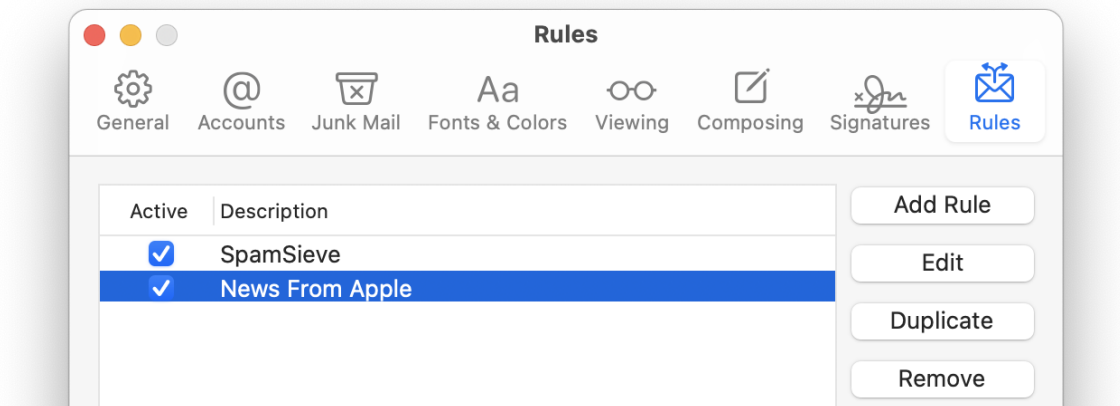




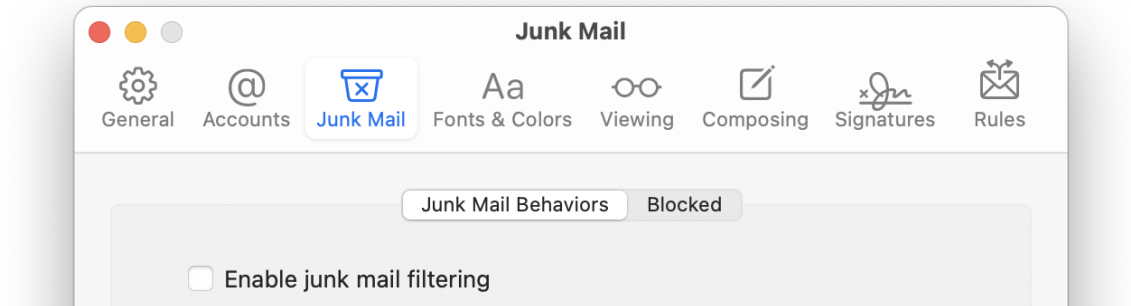
*Note:* Although the rule *looks* like it will move every message to the **Spam** mailbox, because you have installed SpamSieve's plug-in, it will only move the spam messages.

Now click **OK** to close the rule and save your changes. Mail may ask if you want to apply the rule; click **Don't Apply**. (If you were to click **Apply** now, or in the future when editing a rule, that would filter all of the currently displayed old messages through SpamSieve, and you would be obliged to correct any mistakes.)

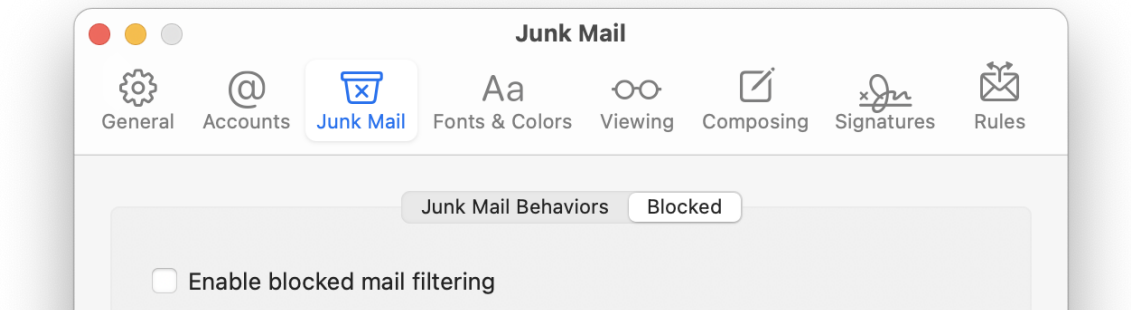
5. Drag the SpamSieve rule to the top of the list so that SpamSieve will be able to filter all of your mail. It's fine to have additional rules in Mail for processing your good messages. Just make sure that they are below the **SpamSieve** rule. If you ever need to temporarily disable SpamSieve, e.g. for testing purposes, you can do so simply by unchecking the rule.



6. Make sure that the list shows no other rules for processing spam/junk messages. If you find any, disable them (by unchecking them) or delete them.
7. Go to the **Junk Mail** tab of Apple Mail's **Preferences** window. If there is a **Trust junk mail headers in messages** option, uncheck it. Uncheck **Enable junk mail filtering** on the **Junk Mail Behaviors** tab. This will disable its junk mail filter so that it doesn't interfere with SpamSieve.



You may also want to uncheck **Enable blocked mail filtering** on the **Blocked** tab. This is because it can be hard to know when to train a SpamSieve mistake if Mail has already deleted the message. SpamSieve's own blocklist automatically works with messages you've trained as spam, and you can set such messages to go [directly to the trash](#) if you want. To block unwanted messages that are not spam, we recommend creating a rule in Mail above the SpamSieve rule.



*Note:* Prior to macOS 10.15, there is no separate **Junk Mail Behaviors** tab—**Enable junk mail filtering** is on the **Junk Mail** tab—and there is no **Enable blocked mail filtering** option.

8. Now it is time to train SpamSieve:
  - To train SpamSieve with spam messages, select one or more of them in Mail and then choose **SpamSieve - Train as Spam** from the **Message** menu. The messages will be colored in gray and moved to the **Spam** mailbox. The [keyboard shortcut](#) for this command is Command-Control-S.

- To train SpamSieve with good messages, select one or more of them and then choose **SpamSieve - Train as Good** from the **Message** menu. If a good message is in the spam mailbox when you train it, it should move to the inbox—otherwise, see [this section](#).

Even with Mail’s built-in junk mail filter disabled, Mail may show a **Not Junk** button [at the top](#) of spam messages; you should ignore this, i.e. always choose **SpamSieve - Train as Good** rather than clicking the **Not Junk** button.

The first time you try to train a message macOS will ask for [permission to control](#) Mail and SpamSieve, and you should click **OK**. When training multiple batches of messages, you should wait for Mail and SpamSieve to finish processing one batch before training the next.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

SpamSieve will process new mail automatically and move the spam messages to the **Spam** mailbox. Mail may still color some messages brown and show them in the special **Junk** mailbox, even though its own junk filter is off; [this is normal](#). The **Junk** mailbox holds spam messages caught by [server-side junk filters](#) before they got to your Mac. These messages are not processed by SpamSieve, so they are not [mistakes](#) and should not be trained as spam. It’s also normal for messages in the **Spam** mailbox to say that you marked them as junk; this is because SpamSieve told Mail that they were junk on your behalf.

If you ever need to manually ask SpamSieve to sift through a mix of spam and good messages, select the messages and choose **Apply Rules** from the **Message** menu. SpamSieve will move the ones that it thinks are spam to the **Spam** mailbox.

The above is all you need to know about using SpamSieve with Mail. The [Apple Mail Customization](#) section explains some more advanced setup options, such as configuring the “new mail” notification sound.

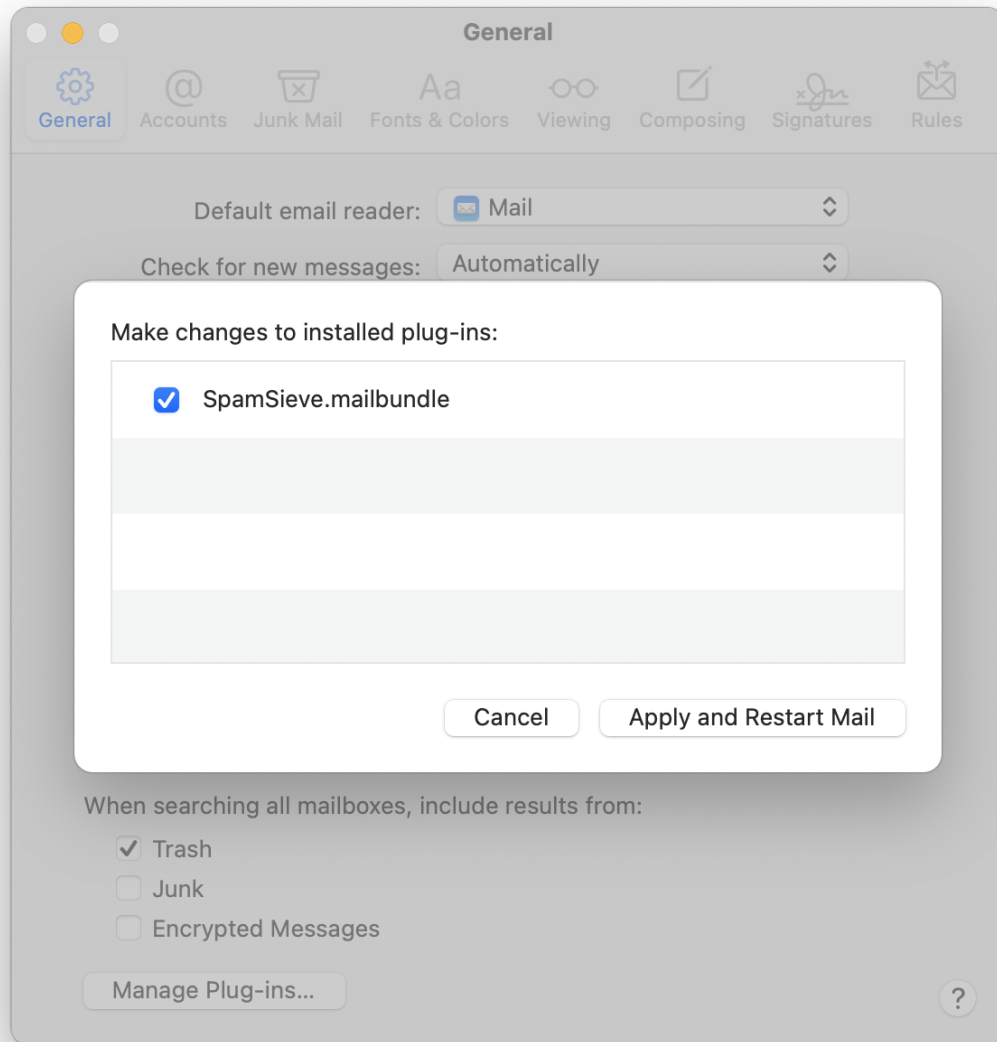
If you need to troubleshoot SpamSieve and Apple Mail, see the [Checking the Apple Mail Setup](#) section and the [Apple Mail-Specific Questions](#) section.

### 3.1.1 Enabling and Updating the Apple Mail Plug-In

After you [install the plug-in](#) for Apple Mail or SpamSieve auto-updates it to a newer version, Mail will not load the plug-in until you enable it. (This is not necessary on macOS 10.13 and earlier.)

#### To Enable the Plug-In

1. Quit Mail if it’s open.
2. Launch Mail and choose **Preferences...** from the **Mail** menu.
3. Click on the **General** tab.
4. Click the **Manage Plug-ins...** button at the bottom of the window.
5. Make sure that **SpamSieve.mailbundle** is checked. Click the **Allow Access** button if Mail asks about that. (If **SpamSieve.mailbundle** isn’t in the list, please see the [If the Apple Mail Plug-In Doesn’t Appear in the List or Doesn’t Stay Enabled](#) section).



6. Click **Apply and Restart Mail**. (If **SpamSieve.mailbundle** was already checked, **Apply and Restart Mail** will be disabled and you can just click **Cancel**.)

### If Mail Reports “Incompatible Plug-ins Disabled”

The newest version of SpamSieve is normally compatible with the newest version of macOS. The latest information about this will be posted on the [support page](#). Sometimes Mail erroneously reports that the SpamSieve plug-in is incompatible because other incompatible plug-ins were found (in that case, just restart Mail) or because of a problem with Mail’s own files (in that case, see [Resetting Mail’s Private Plug-Ins Folder](#)).

## Why the Plug-In Needs to Be Enabled

When you first install the plug-in or when a new version of SpamSieve updates it, Mail will not load the plug-in until you have given your permission by enabling it.

If SpamSieve's Mail plug-in is not loaded, Mail will not filter new messages through SpamSieve, and you will not be able to train SpamSieve. Additionally, if Mail receives new messages while the SpamSieve plug-in is disabled, the **SpamSieve** rule in Mail will move them to the **Spam** mailbox [without consulting SpamSieve](#). SpamSieve will try to prevent this by temporarily deactivating the rule if it notices that the plug-in is disabled. You can also do this yourself by unchecking the **SpamSieve** rule in Mail's preferences before updating SpamSieve. Or you can just drag the messages back to the inbox if you happen to receive any before you've had a chance to re-enable the plug-in. (They do not need to be trained as good because SpamSieve did not think they were spam; they were moved by Mail.)

## If You No Longer Want to Use Apple Mail With SpamSieve

If you've switched to another mail client and don't want SpamSieve to remind you to enable its Mail plug-in, choose [Uninstall Apple Mail Plug-In. . .](#) from [the SpamSieve menu](#) to tell SpamSieve that you are no longer using Mail.

## Troubleshooting

Please see:

- [If the Apple Mail Plug-In Doesn't Appear in the List or Doesn't Stay Enabled](#)
- [If SpamSieve Tells You the Apple Mail Plug-In Isn't Loading, But It Is](#)
- [Resetting Mail's Private Plug-Ins Folder](#)

## 3.2 Setting Up Airmail

These instructions apply to version 4 of Airmail. For older versions of Airmail, please see the [Setting Up Airmail 1–3](#) section.

1. Make sure that you are using 4.0 or later.
2. From the **Airmail** menu, choose **Preferences. . .**
3. Click on the **Accounts** icon at the top of the window. For each IMAP or Gmail account in the list:
  - a) Click on the gear icon, then the **More** tab.
  - b) Make sure **Message Content** is checked.
  - c) Make sure **Attachments** is checked.

POP accounts do not have the **Download** section, so you can skip this step for them.

Click the **Save** button.

4. Click on the **Advanced** icon at the top of the window and make sure that **Use SpamSieve** is checked.

5. Now it is time to train SpamSieve:

- To train SpamSieve with spam messages, select the messages, Control-click, and choose **SpamSieve - Train as Spam** from the contextual menu. (Do not use the **Mark as Spam** command.) You can also choose **Messages ▸ Mark as Reminder ▸ Spam Sieve - Train as Bad** or press the Option-Shift-Command-B keyboard shortcut.
- To train SpamSieve with good messages, select the messages, Control-click, and choose **SpamSieve - Train as Good** from the contextual menu. (Do not use the **Mark as Not Spam** command.) You can also choose **Messages ▸ Mark as Reminder ▸ Spam Sieve - Train as Good** or press the Option-Shift-Command-G keyboard shortcut.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

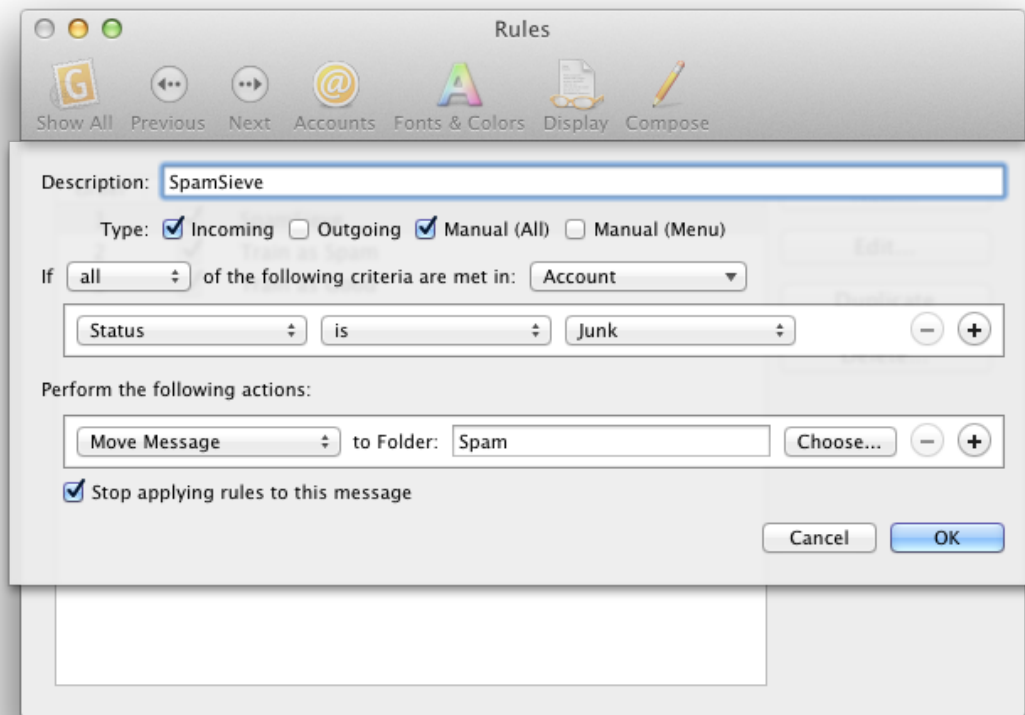
On macOS 10.14 or later, the first time you try to train a message macOS will ask whether Airmail [can control](#) SpamSieve, and you should click **OK**.

SpamSieve will process new mail automatically. Messages that it thinks are spam will be moved to the **Junk** or **Spam** folder. Airmail will automatically launch SpamSieve when there are new messages that need to be filtered or when you train messages as spam or as good.

If you need to troubleshoot SpamSieve and Airmail, see the [Checking the Airmail Setup](#) section.

### 3.3 Setting Up GyazMail

1. 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**.
2. By default, GyazMail will color the incoming 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. Now it is time to train SpamSieve:

- To train SpamSieve with spam messages, select the messages, go to GyazMail's **Message** menu, and choose **Junk** ▸ **Mark as Junk**.
- To train SpamSieve with good messages, select the messages, go to GyazMail's **Message** menu, and choose **Junk** ▸ **Mark as Not Junk**.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

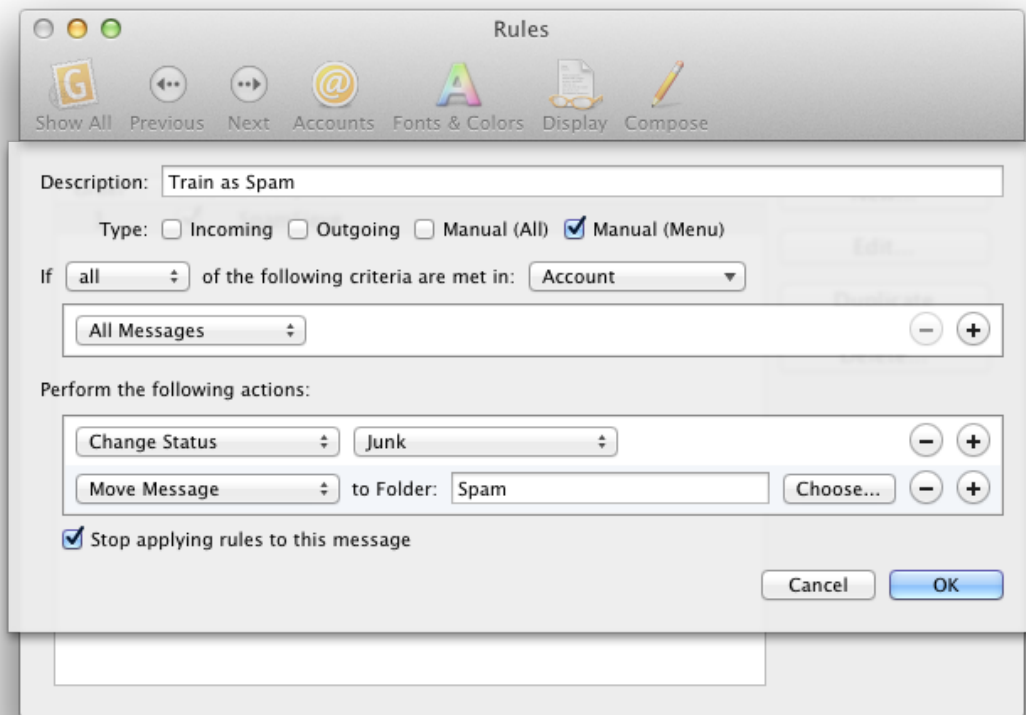
You can also use the **Junk** button on the toolbar or the **Message** ▸ **Status** ▸ **Junk** menu command to toggle the junk status of the selected messages.

SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **Junk** ▸ **Recheck Junk Status** from the **Message** menu.

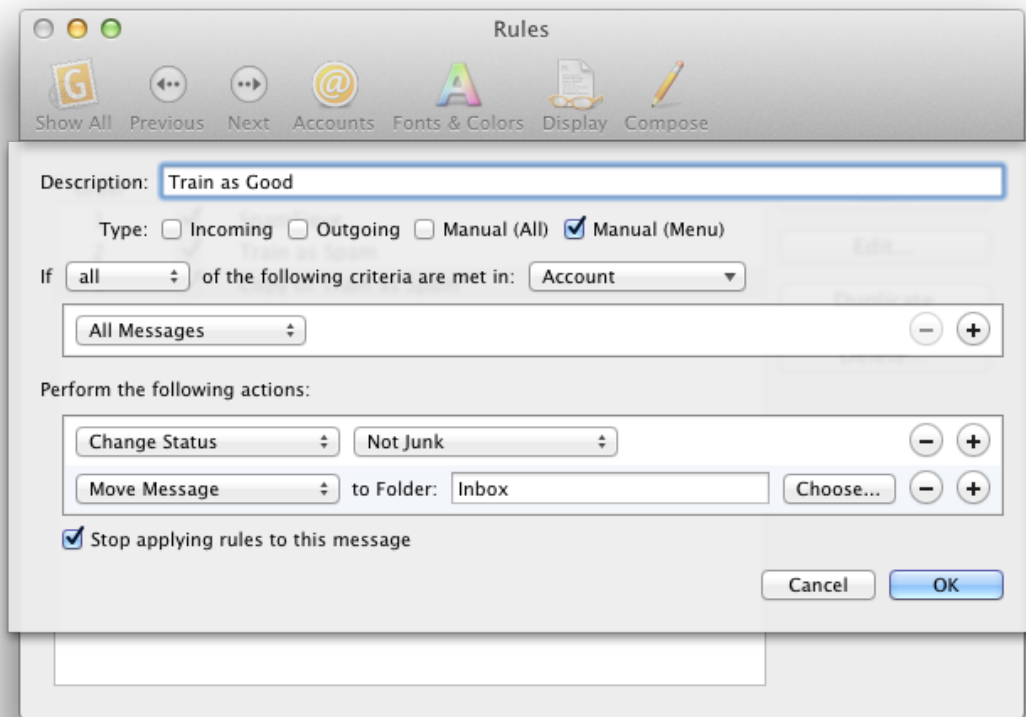
If you need to troubleshoot SpamSieve and GyazMail, see the [Checking the GyazMail Setup](#) section.

### Moving Trained Messages

Normally, when you mark a message as junk or not junk in GyazMail, the message stays in the same mailbox. If you would like spam messages to move to the **Spam** mailbox and good messages to move to the inbox, you can set up two rules like this:







Then, instead of using the **Junk** and **Not Junk** buttons to train messages, you can use the **Message** ▸ **Apply Rule** ▸ **Train as Spam** and **Message** ▸ **Apply Rule** ▸ **Train as Good** menu commands to train and move them at the same time.

If desired, you can set up keyboard shortcuts for training. For example, give the **Train as Spam** rule a keyboard shortcut of Command-Control-S, change the **Description** of the rule to **Train as Spam**\@<sup>^</sup>s.

### 3.4 Setting Up MailMate

1. Make sure that you are using MailMate 1.1.2 or later.
2. In MailMate's **Security** preferences, make sure that **Enable** is checked next to **SpamSieve** and that **Enable for messages in** is set to **Inbox**.
3. The **Mark messages as Not Junk if score is below** setting does not affect SpamSieve or its filtering. Rather, if SpamSieve thinks a message is less spammy than the score that you enter, MailMate will tell the mail server that it's not junk, and it will also decide that it's safe to display any remote images that the message references. If you would like to see remote images for all the messages that SpamSieve thinks are good, you should set this to 50.
4. Now it is time to train SpamSieve:

- To train SpamSieve with spam messages, select the messages and click the **Move to Junk** button, or choose **Message ▸ Junk State ▸ Junk** from the menu bar, or move the message to the **Junk** mailbox.
- To train SpamSieve with good messages, select the messages and click the **Not Junk** or **Move Out of Junk** button, or choose **Message ▸ Junk State ▸ Not Junk** from the menu bar, or move the message out of the **Junk** mailbox.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

SpamSieve will process new mail automatically. The **SpamSieve Score** column shows how spammy SpamSieve thought each message was, on a scale from 0 to 100 (with 50 and above meaning spam). (The **Spam Score** column shows the spam level reported by the server junk filter, if any.)

If you ever need to manually ask SpamSieve to sift through a mix of spam and good messages, choose **Junk State ▸ SpamSieve ▸ Evaluate** from the **Message** menu. (The **Recompute Score** command is similar except that it only updates the **SpamSieve Score** column in MailMate’s display. It does not move spam messages to the **Junk** mailbox.)

*Note:* On macOS 10.14 or later, the system will prompt you in order to let MailMate control SpamSieve, and you should allow this. For more information, see the [Security & Privacy Access](#) section.

If you need to troubleshoot SpamSieve and MailMate, see the [Checking the MailMate Setup](#) section.

### Filtering Other Mailboxes

The above setup will automatically filter new messages that arrive in the inbox. If you have new messages in other mailboxes, e.g. due to server filtering rules or SaneBox, you can:

1. Choose **Mailbox ▸ New Smart Mailbox...**
2. Click the **+** button and add each additional mailbox that you would like to be filtered.
3. In the **Preferences ▸ Security** window, set **Enable for messages in** to the smart mailbox that you just created.

## 3.5 Setting Up Mailsmith

1. Open Mailsmith’s **Preferences** window and click on the **Spam Handling** pane. Make sure that **Use SpamSieve** is checked. Uncheck **Honor SpamAssassin** and **BogoFilter** headers.
2. Now it is time to train 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.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

If you ever need to manually ask it to sift through a mix of spam and good messages, choose **Recalculate Spam Score** from the **Message** menu.

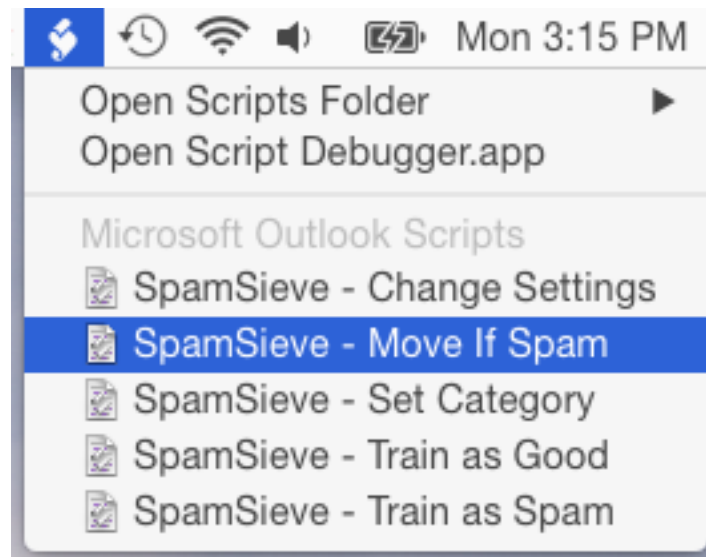
The above is all you need to know about using SpamSieve with Mailsmith. For more information about using SpamSieve with Mailsmith, please see Chapter 8 of the Mailsmith User Manual.

If you need to troubleshoot SpamSieve and Mailsmith, see the [Checking the Mailsmith Setup](#) section.

### 3.6 Setting Up Outlook

These instructions apply to Microsoft Office 365 (also known as Outlook 2016 and Outlook 2019, versions 15.x and 16.x). The “[New Outlook](#)” switch at the top of the window needs to be **Off**, as the in-progress “new look” version of Outlook [does not support AppleScript](#). For older versions of Outlook, please see the [Setting Up Outlook 2011](#) section.

1. In the Finder, choose **Utilities** from the **Go** menu and open the Script Editor (or AppleScript Editor) application. Open its **Preferences** window. Click on the **General** tab, and make sure that **Show Script menu in menu bar** is checked. (You may have to uncheck and then check the box before the icon shows up in the menu bar.)
2. Switch to SpamSieve by clicking on its icon in the Dock. Go to the **SpamSieve** menu and choose **Preferences...** Make sure that [Use Entourage/Outlook address book](#) is checked and click the **Load** button, then the **Outlook** button.
3. Choose **Install Outlook Scripts** from the **SpamSieve** menu. When in Outlook, you should now see five SpamSieve items in **Script** menu at the top-right of your screen:

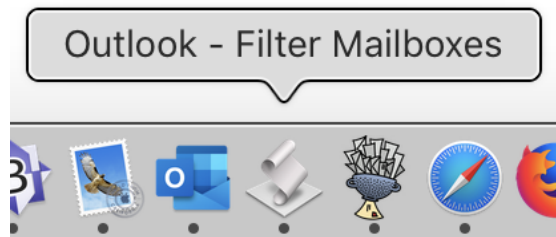


4. You will now create an **InboxSpamSieve** folder in each account and set up a rule to move new messages to that folder. SpamSieve will periodically scan the messages in this folder, moving the good ones to **Inbox** and the spam ones to **Junk**.
  - For each IMAP or Exchange account that you have, follow the [Outlook IMAP/Exchange Account Rules](#) instructions.

- For each Gmail account that you have, follow the [Outlook Gmail Account Rules](#) instructions.
- For each POP account that you have, follow the [Outlook POP Account Rules](#) instructions.

5. Install the **Outlook - Filter Mailboxes** helper application. To do this:

- Click [this link](#) to download the Outlook - Filter Mailboxes.dmg file.
- Open the Outlook - Filter Mailboxes.dmg file and drag the Outlook - Filter Mailboxes.app file to your Applications folder. If it asks whether you want to replace an existing item, click **Replace** to replace the old version with the new version.
- Drag the Outlook - Filter Mailboxes.dmg file to the trash.
- Double-click the Outlook - Filter Mailboxes.app file in your Applications folder.



- You will need to launch this application whenever you want SpamSieve to monitor Outlook for new messages that need to be filtered.* You can optionally set up Outlook - Filter Mailboxes.app as a **Login Item** in the **Users & Groups** section of System Preferences if you want it to launch automatically. The easiest way to do this is to click and hold on its Dock icon and make sure that **Options** ▸ **Open at Login** is checked.

6. Now it is time to train SpamSieve:

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

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

*Note:* On macOS 10.14 or later, the first time you try to train a message macOS will ask for [permission to control](#) Outlook and SpamSieve, and you should click **OK**.

SpamSieve will process new mail automatically every minute, moving good messages to your inbox and spam messages to the **Junk** folder. Prior to Outlook 15.36, Outlook had a single top-level folder called **Junk Email**, with per-account folders inside. In Outlook 15.36, there is a separate **Junk** folder within the section for each account. For more information, please see [this thread](#).

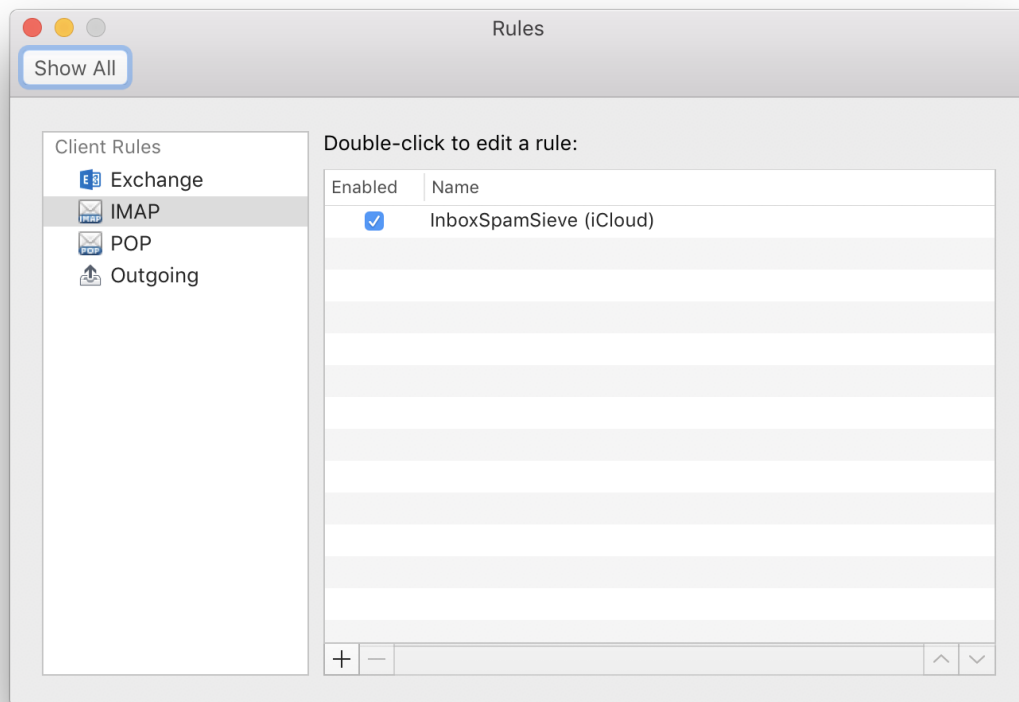
Messages yet to be processed will be held in the **InboxSpamSieve** folders. You can make it process the messages immediately by clicking on the **Outlook - Filter Mailboxes** icon in the Dock. If you ever need to manually ask SpamSieve to sift through a mix of spam and good messages, select the messages and choose **SpamSieve - Move If Spam** from the **Script** menu.

The above is all you need to know about using SpamSieve with Outlook. The [Outlook Customization](#) section explains some more advanced setup options. If the filtering doesn't seem to be working properly, you can check the setup as described in the [Checking the Outlook Setup](#) section.

### 3.6.1 Outlook IMAP/Exchange Account Rules

When [Setting Up Outlook](#), repeat these instructions for each IMAP and Exchange account that you have:

1. Create a new folder called **InboxSpamSieve** in the account. You can do this by Control-clicking on the name of the account in Outlook's main window and choosing **New Folder**.
2. Go to Outlook's **Tools** menu and choose **Rules** to open the **Rules** list.



3. Click on the source list item under **Client Rules** corresponding to the type of account you that have (e.g. **IMAP** or **Exchange**). Ignore the **Server Rules** section of the window, if any.
4. Uncheck or delete any (non-SpamSieve) rules for filtering out junk/spam e-mails.
5. Click the **+** button at the bottom of the window to create a new rule.
6. Change the name of the rule to **InboxSpamSieve (AccountName)** where **AccountName** is the name of your account (e.g. **iCloud** in this example).
7. Under **When a new message arrives**, choose **Folder**, **Is**, and **INBOX (AccountName)**:

Rule name:

When a new message arrives: If any conditions are met

Folder Is INBOX (iCloud)


Do the following:


Move Message InboxSpamSieve (iCloud)


☒ Do not apply other rules to messages that meet these conditions


☒ Enabled Cancel OK


If **INBOX (AccountName)** is not in the third pop-up menu, you can select **Choose Folder...** from the pop-up menu and then search for it by typing **Inbox**:


 **Inbox**  
Gmail/Inbox

 **INBOX**  
iCloud/INBOX

 **InboxSpamSieve**  
Gmail/InboxSpamSieve

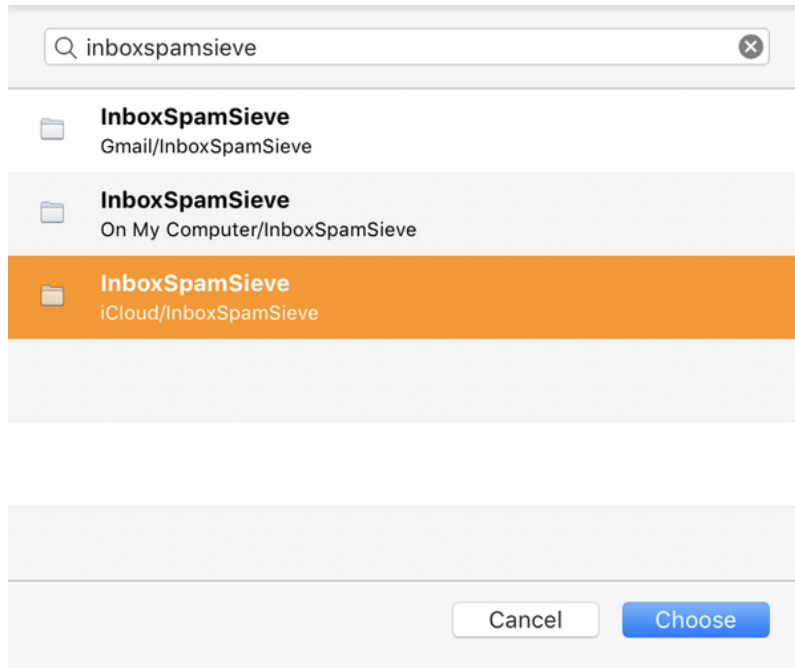
 **InboxSpamSieve**  
On My Computer/InboxSpamSieve

 **InboxSpamSieve**  
iCloud/InboxSpamSieve

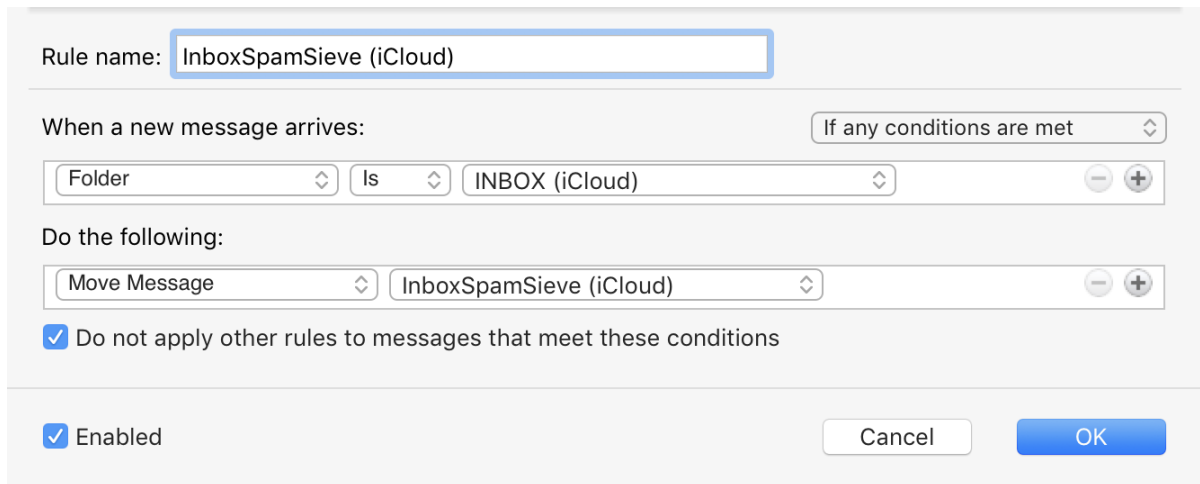
 **Inbox**  
On My Computer/Inbox

Cancel Choose

8. Under **Do the following**, choose **Move Message** and **InboxSpamSieve (AccountName)**. If **InboxSpamSieve (AccountName)** is not in the second pop-up menu, you can choose **Choose Folder...** from the pop-up menu and then search for it by typing **InboxSpamSieve**:



9. The rule should now look like:



Click **OK** to save the rule.

10. In Outlook's **Preferences** > **Accounts** window, select the account in the list and click **Advanced...** In the **Server** tab, make sure that **Sync all IMAP folders every \_ minutes** is checked. We recommend setting it to a small number, such as 2. (You can skip this step if you're using an Exchange account rather than an IMAP one.)
11. You can now repeat this section for any additional IMAP or Exchange accounts, or return to [Setting Up Outlook](#) at Step 5.

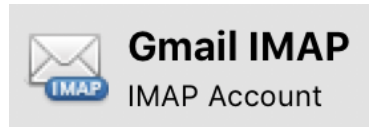
### 3.6.2 Outlook Gmail Account Rules

When [Setting Up Outlook](#), repeat these instructions for each Gmail account that you have.

#### Gmail Account Types in Outlook

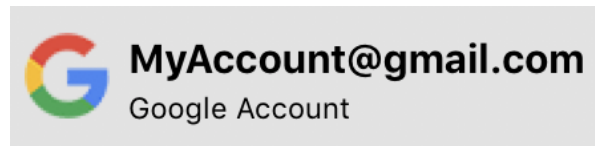
A Gmail account in Outlook can be set up in two different ways:

1. It can be treated as a generic **IMAP account**. Such accounts look like this in Outlook's **Accounts** preferences:



Prior to Outlook version 16.17, this was the only option, so it's likely what you have if you originally set up your account using an older version of Outlook.

2. It can be set up as a special **Google account**. Such accounts look like this in Outlook's **Accounts** preferences:



This option is only possible with newer versions of Outlook. Using the Google account type enables some Gmail-specific calendar and contacts features in Outlook. However, we generally recommend using an IMAP account instead, due to various limitations and bugs with Google accounts in the current version of Outlook.

#### Setting Up SpamSieve With a Gmail IMAP Account

SpamSieve works best when a Gmail account is set up as a generic IMAP account. To set up an account to use IMAP:

1. From the **Outlook** menu, choose **Preferences** and then click on **Accounts**.
2. If your account does not already appear in the list, skip to Step 3. If your Gmail account was already set up as a Google account, you can remove it by selecting it and clicking the - button.
3. Click the + button and choose **New Account...**
4. Enter your Gmail e-mail address and click **Continue**.
5. Click the **Not Google?** button at the top of the window.
6. Click **IMAP/POP**, fill in the rest of the information, and click **Add Account**.
7. Now follow the regular [Outlook IMAP/Exchange Account Rules](#) instructions to set up Outlook to filter the account with SpamSieve.

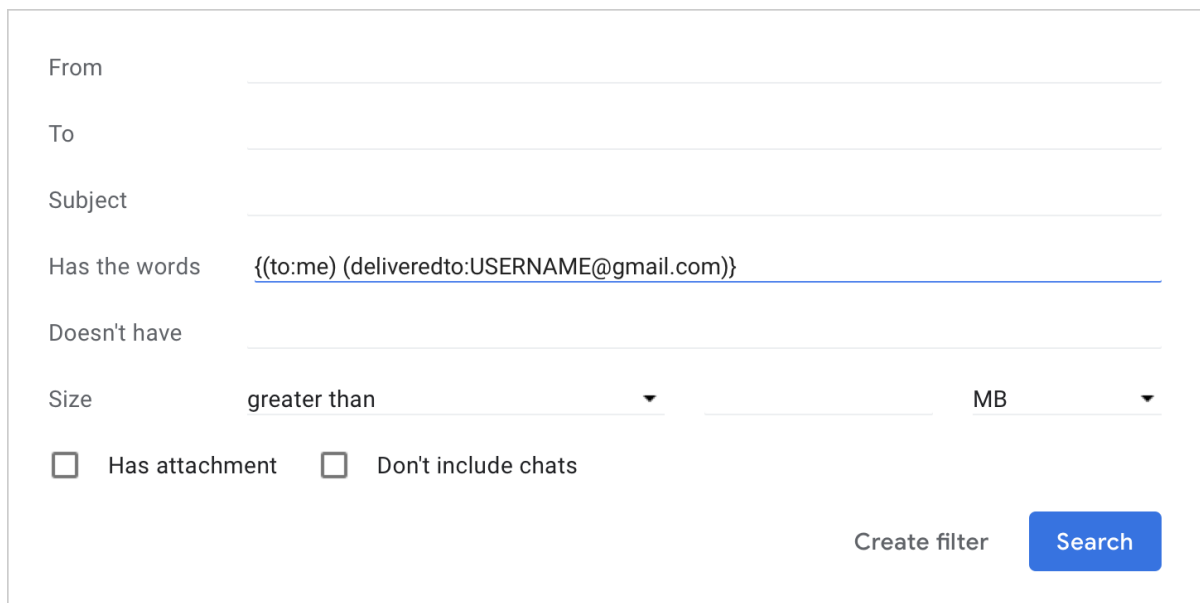


## Setting Up SpamSieve With a Gmail Google Account

We recommend using the IMAP setup (above) where possible because, if you have multiple accounts, Outlook may move Google messages to the **Inbox** or **Junk Email** mailbox of the wrong account.

However, if you need to set up your Gmail account as a Google account in Outlook, it is still possible to use SpamSieve:

1. Log into the Gmail Web site.
2. Create a new label (folder) called **InboxSpamSieve**. The **+ Create new label** command is located at the left of the window. You may need to click **More** in order to see it.
3. Click the gear at the top right, choose **Settings**, then click on **Filters and Blocked Addresses**.
4. Click **Create a new filter**. Enter `{(to:me) (deliveredto:USERNAME@gmail.com)}` in the **Has the words** field (replacing USERNAME with your actual Gmail username).



From \_\_\_\_\_

To \_\_\_\_\_

Subject \_\_\_\_\_

Has the words `{(to:me) (deliveredto:USERNAME@gmail.com)}`

Doesn't have \_\_\_\_\_

Size greater than MB

☐ Has attachment ☐ Don't include chats

Create filter [Search](#)

Then click **Create filter**.

5. Check the **Skip the Inbox (Archive it)** and **Apply the label** boxes and select **InboxSpamSieve** as the label.

← When a message arrives that matches this search:

- ☒ Skip the Inbox (Archive it)
- ☐ Mark as read
- ☐ Star it
- ☒ Apply the label: InboxSpamSieve ▼
- ☐ Forward it [add forwarding address](#)
- ☐ Delete it
- ☐ Never send it to Spam
- ☐ Always mark it as important
- ☐ Never mark it as important
- ☐ Categorize as: Choose category... ▼
- ☐ Also apply filter to matching conversations.

? [Learn more](#)

Create filter

*Note:* This will cause spam messages to be temporarily moved to Gmail's archive, however they should be automatically removed from the archive when you delete them from Outlook. For more information, see [Keeping Spam Messages Out of Gmail's Archive](#), which shows how to have Gmail not archive messages that are deleted via IMAP.

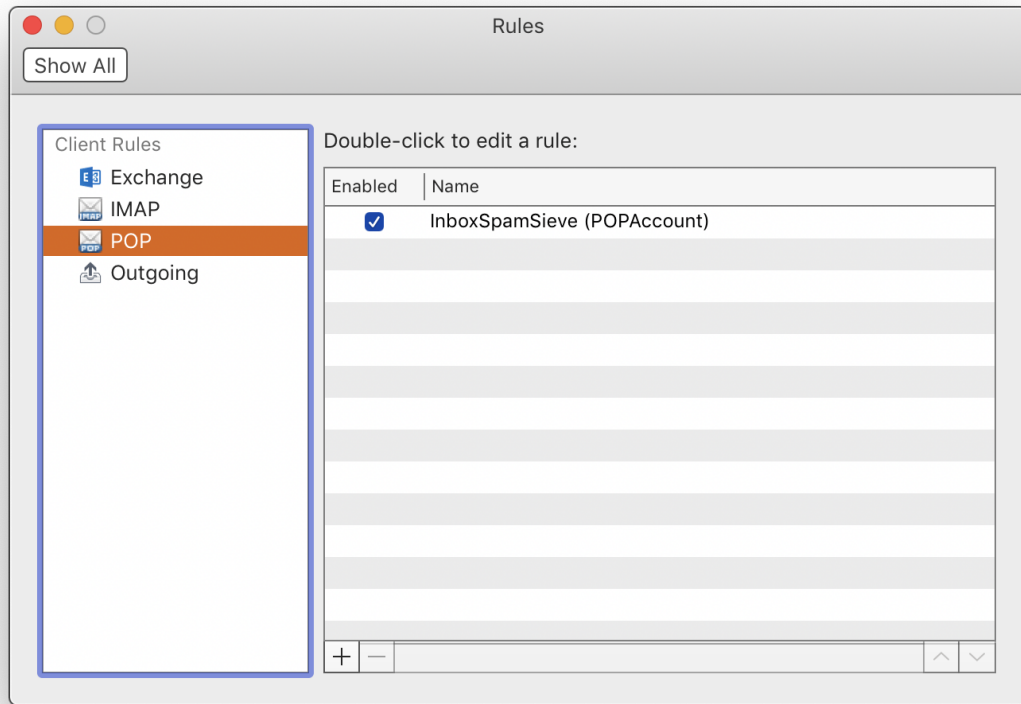
6. Click **Create filter**.

You can now repeat this section for any additional Gmail accounts, or return to [Setting Up Outlook](#) at Step 5.

### 3.6.3 Outlook POP Account Rules

When [Setting Up Outlook](#), repeat these instructions for each POP account that you have.

1. Create a new folder called **InboxSpamSieve**. You can do this by Control-clicking on **On My Computer** in Outlook's main window and choosing **New Folder**. (You only need one folder for all your POP accounts.)
2. Go to Outlook's **Tools** menu and choose **Rules** to open the **Rules** list.



3. Click on **POP** under **Client Rules**.
4. Uncheck or delete any (non-SpamSieve) rules for filtering out junk/spam e-mails.
5. Click the **+** button at the bottom of the window to create a new rule.
6. Change the name of the rule to **InboxSpamSieve (AccountName)** where **AccountName** is the name of your account (e.g. **POPAccount** in this example).
7. Under **When a new message arrives**, choose **Account**, **Is**, and **AccountName** (iCloud in this example):

Rule name:

When a new message arrives: If any conditions are met

Account Is iCloud

Do the following:

Move Message InboxSpamSieve (On My Computer)

☒ Do not apply other rules to messages that meet these conditions

☒ Enabled Cancel OK

8. Under **Do the following**, choose **Move Message** and **InboxSpamSieve (On My Computer)**. If **InboxSpamSieve (On My Computer)** is not in the second pop-up menu, you can choose **Choose Folder...** from the pop-up menu and then search for it.
9. Click **OK** to save the rule. You can now repeat this section for any additional POP accounts, or return to [Setting Up Outlook](#) at Step 5.

### 3.7 Setting Up Postbox

*Note:* These instructions apply to Postbox 2.x through 5.x. Postbox 6 and 7 do not currently have [direct support](#) for SpamSieve, but you can use it by following the [Setting Up Other Mail Clients](#) instructions.

1. Choose **Install Postbox Plug-In** from SpamSieve's **SpamSieve** menu.
2. Launch Postbox. Choose **Add-ons** from the **Tools** menu.
3. If you have Postbox 2.5 or later, click on the action (gear) menu in the upper-right corner of the window and choose **Install Add-on From File...** If you have Postbox 2.0, click the **Install...** button in the window that just opened.
4. In the file open panel, find your **Downloads** folder, select the **SpamSieveForPostbox.xpi** file, and click **Open**.
5. Click the **Install Now** button.
6. Quit Postbox and re-launch it. If you now go to the **Tools** menu and choose **Add-ons** you should see the **SpamSieve Postbox 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 **SpamSieveForPostbox.xpi** file from your desktop.
7. Choose **Preferences...** from the **Postbox** menu and click on **Accounts**. For each of your accounts in the list at the left (plus **On My Mac**), click on **Junk Settings** and make sure that:
  - **Enable adaptive junk mail controls for this account** is checked.
  - **Move new junk messages to** is checked.
  - **Trust junk mail headers set by** is unchecked.

It is generally a good idea to uncheck the items under “Do not mark mail as junk if the sender is in” since these can prevent SpamSieve from filtering out certain spam messages.

8. Choose **Preferences...** from the **Postbox** menu and click on **Privacy**. Make sure that **When I mark messages as junk** is checked.

9. Now it is time to train SpamSieve:

- To train SpamSieve with spam messages, select one or more of them and then choose **Message** ▸ **Mark** ▸ **As Junk**, click the bullet in the junk status column of the message list, or press the J key.
- To train SpamSieve with good messages, select one or more of them and then choose **Message** ▸ **Mark** ▸ **As Not Junk**, click the junk icon in the junk status column of the message list, or press the J key.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

You can also customize the toolbar to add a **Junk/Not Junk** button.

*Note:* If Postbox already thinks that a message is junk, it may not let you mark it as junk—also likewise for not junk. That’s OK; it is enough to train SpamSieve by marking the messages that are misclassified in Postbox.

SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **Message** ▸ **Mark** ▸ **Run Junk Mail Controls**.

The above is all you need to know about using SpamSieve with Postbox. The [Customization](#) section explains some more advanced setup options.

If you need to troubleshoot SpamSieve and Postbox, see the [Checking the Postbox Setup](#) section.

### 3.8 Setting Up PowerMail

These instructions apply to PowerMail 6 and PowerMail 5. Please see the [Setting up PowerMail 4](#) section if you need to setup an older version of PowerMail.

1. Make sure that you are using a POP (not IMAP) account.
2. 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.
3. Now it is time to train 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.

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **Perform Filter** ▸ **Perform All Filters** from the **Mail** menu.

The above is all you need to know about using SpamSieve with PowerMail. The [Customization](#) section explains some more advanced setup options. For more information about how to configure PowerMail's handling of spam messages, please see the PowerMail documentation.

If you need to troubleshoot SpamSieve and PowerMail, see the [Checking the PowerMail Setup](#) section.

### 3.9 Setting Up Gmail, iCloud, Yahoo, AOL, or Other Web Mail

SpamSieve works with Web mail accounts, provided that they allow access via POP, IMAP, or Exchange. This includes Gmail, iCloud, Yahoo, [AOL](#), Outlook.com, and most other Web mail providers. Just configure Apple Mail to access your account and then follow the normal SpamSieve setup instructions in the [Setting Up Apple Mail](#) section. SpamSieve will then filter your Web mail when Apple Mail is running.

You can train SpamSieve from within Apple Mail. If you use the [drone setup](#), you can also train SpamSieve from your Web browser by moving messages into the special training mailboxes.

See also:

- [Keeping Spam Messages Out of Gmail's Archive](#)
- [Hiding Special Gmail Mailboxes From IMAP](#)
- [How should I configure the junk filter on my mail server?](#)

### 3.10 Setting Up Other Mail Clients

You can still use SpamSieve with mail programs that are not [directly supported](#). To do this, configure Apple Mail to access your mail account and then follow the normal SpamSieve setup instructions in the [Setting Up Apple Mail](#) section. SpamSieve will then filter your Web mail when Apple Mail is running. It can run in the background—and you can hide its windows if desired—while you use your preferred mail client to perform your normal e-mail tasks. (To do this automatically, you can set up Apple Mail in **System Preferences** ▸ **Users & Groups** ▸ **Login Items** and click the **Hide** checkbox.)

You can train SpamSieve from within Apple Mail or use the [drone setup](#) to train SpamSieve from your primary mail client by moving messages into the special training mailboxes.

### 3.11 Do an Initial Training

SpamSieve does not have distinct “training” and “working” modes. As soon as you install it, it is always learning from the messages it sees and always filtering out the spam that it finds.

Although you can start using SpamSieve immediately and just [correct any mistakes](#) that it makes, it will do a better job of filtering if you use some of your old mail to do an initial training. This simply means

that you give it some examples of messages you consider to be spam, and ones which you do not. You do this by selecting some messages in your mail program and choosing a training command from the menu (as described in the last step of the [“Setting Up”](#) section for your mail program). SpamSieve collects information from the messages it’s trained with into its [corpus](#), which it uses to predict whether subsequent messages are spam. Don’t worry; it learns quickly!

How many messages you should train SpamSieve with depends on how many old messages you have and on how much time you want to put into the process. 195 spam messages and 105 representative good ones are enough for most people to get very good accuracy, but it’s OK if you don’t have that many. The important points are:

**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.**

For example, use 650 spams and 350 good messages or 65 spams and 35 good messages. It is better to use fewer messages in the initial training (i.e. not use all your saved mail) than to deviate from the recommended percentage. For example, if you have 500 good messages but only 195 saved spam messages, don’t train SpamSieve with all 695 messages. Instead, train it with the 195 spams and about 105 representative good messages.

In order to monitor your progress, you can go to SpamSieve’s **Filter** menu and choose [Show Statistics](#). The **Corpus** section in the middle 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.

After the initial training, you don’t have to worry about the number or percentage of messages in the corpus. SpamSieve will automatically learn from new messages as they arrive and keep its corpus properly balanced.

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.

Now you’re done setting up SpamSieve. The [Correct All Mistakes](#) section explains how you can keep SpamSieve’s accuracy high by telling it if it puts any messages in the wrong mailbox.

## 3.12 Correct All Mistakes

SpamSieve examines each incoming message and moves the spam messages into a separate spam mailbox. It leaves the good messages alone, so they will stay in the inbox or be processed by your other mail rules. In order to keep SpamSieve’s accuracy high, you’ll need to correct any mistakes that it makes:

- If you find a spam message that’s not in the spam mailbox, train it as spam.

- If you find a good message in the spam mailbox, train it as good.

Normally, the [Train SpamSieve whitelist](#) and [Train SpamSieve blocklist](#) preferences are enabled. This means that training a single message as good will make SpamSieve classify all future messages from that message's sender as good. Likewise, training a message as spam will make SpamSieve classify all future messages from that message's sender as spam. Normally, the [Train Bayesian classifier](#) preference is also enabled, which will let SpamSieve learn from the message's *contents* so that it can recognize future messages that are *similar* even if the sender is different.

## How to Correct Mistakes

To correct a mistake, train SpamSieve using the menu commands recommended at the end of the [“Setting Up” section of the manual](#) for your mail program. For example, with Apple Mail you would select the message and choose **SpamSieve - Train as Good** or **SpamSieve - Train as Spam** from Mail's **Message** menu. Always train SpamSieve using the menu commands. Do not move the messages into or out of the spam mailbox yourself, as this will bypass SpamSieve.

## Correcting All the Mistakes

You must correct *all* of SpamSieve's mistakes or its accuracy will deteriorate over time. The reason for this is that SpamSieve assumes that it classified a message correctly unless you tell it otherwise, and it will learn based on that assumption (unless you turn off the [Auto-train with incoming mail](#) preference). Also, the *sooner* you correct SpamSieve, the better. By [promptly](#) correcting SpamSieve, you ensure that it's always acting based on accurate information.

## Which Messages to Train

After the [initial training](#), it is not necessary (or recommended) to train SpamSieve with messages that are not mistakes.

- *Do train* all the spam messages that get through to your inbox. Do this even for phishing messages, image spams, and messages from forged senders that you might think would confuse SpamSieve. It's best to [tell SpamSieve the truth](#). Don't delete spam messages from your iPhone's inbox because that would prevent you from training them as spam on the Mac.
- *Do not train* messages that SpamSieve automatically put in the spam mailbox. Regardless of which [color of spamminess](#) it assigned them, SpamSieve already thinks that they are spam.
- *Do not train* messages that a [server filter](#) automatically caught in the **Junk** mailbox or **Bulk Mail** mailbox.
- *Do not train* as spam messages that are merely unwanted, i.e. messages from:
  - Legitimate mailing lists that you no longer wish to read.
  - Companies that you have done business with.
  - People that you know who send or forward annoying messages.

These messages are not spam, so training them as such could confuse SpamSieve. For mailing lists, there should be instructions at the bottom of the e-mail to unsubscribe. Social media sites have ways that you can configure which types of messages they send you. For other types of unwanted messages, see you can optionally create a rule in your mail program [above the SpamSieve rule](#) to move or delete them before SpamSieve sees them.



- *Do not train* quarantine digests from a server spam filter. These messages are not spam, but they contain lots of spammy words. It's best to either [turn off](#) the server spam filter or to create a rule in your mail program *above the SpamSieve rule* to move these messages to another mailbox before SpamSieve sees them.
- *Do not train* messages in Gmail's **All Mail**, **Important**, or **Starred** mailboxes as spam, as these messages are duplicates not filtered by SpamSieve. For more information, see the [Setting Up Gmail, iCloud, Yahoo, AOL, or Other Web Mail](#) section of the manual.
- *Do not delete* unwanted [whitelist](#) or [blocklist](#) rules that SpamSieve auto-created. Instead, let SpamSieve automatically disable the matching rules when you train messages as spam or as good.

## Undoing a Training

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

## Disable Other Spam Filters and Rules

When using SpamSieve, turn off any other spam filters that you've installed on your Mac. Disable any manual rules that you've created that move messages to the **Spam** mailbox or trash. This will make it clear which messages SpamSieve did and didn't catch, which is necessary for you to be able to properly correct it. If you really need those manual rules, you can recreate them using SpamSieve's [blocklist](#) or put the rules above SpamSieve's rule(s) so that the messages are moved or deleted before SpamSieve sees them.

## Using SpamSieve With Multiple Macs

Please see the [SpamSieve and Multiple Macs](#) section for information about how to ensure that you are properly correcting mistakes when multiple copies of SpamSieve are filtering the same mail account.

## Resetting SpamSieve

Not correcting all the mistakes will cause SpamSieve to learn incorrect information, which will reduce the filtering accuracy. The only way to fix this is to reset all of SpamSieve's training:

1. Quit SpamSieve and your mail program.
2. Open the [Library folder](#) and drag the SpamSieve folder to the trash:

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

3. Follow the instructions in the [Do an Initial Training](#) section.

## 3.13 SpamSieve and Multiple Macs

If you are accessing the same IMAP or Exchange mail account from multiple Macs running SpamSieve, it can be difficult to know which copy of SpamSieve needs to be trained to [correct a mistake](#). There are several ways to deal with this (in order of preference):

1. Run SpamSieve on a single Mac and let it clean your inbox for [all the Macs](#). All the training is done from that Mac. This is the simplest solution. It works well when the Mac with SpamSieve will be running most of the time, and when you can easily access that Mac to do the training.
2. Run SpamSieve on a single Mac using the [drone setup](#). This setup works well when the Mac with SpamSieve will be running most of the time. When you're away from that Mac, you can remotely train SpamSieve from any Mac, iOS device, or even via Web mail.
3. Run SpamSieve on all the Macs and uncheck the [Auto-train with incoming mail](#) preference (on all the Macs). You can train whichever Mac you happen to be using at the moment. This will have lower filtering accuracy than (1) or (2) but is useful in situations when you do not have a single Mac that is always available for mail filtering. With auto-training off, you may find it especially helpful to enable [whitelisting of previous recipients](#).
4. Run SpamSieve on all the Macs, being careful to only let one copy of SpamSieve run at a time, and to always correct all the mistakes before switching to another Mac. This will give better filtering accuracy than (3) but is a lot more work.

## Server Spam Mailbox

With the normal setup, spam messages are stored locally, so they are only accessible on one Mac. If you are using multiple Macs, you can instead [store the spam on the server](#) so that the same spam mailbox is visible on all the Macs.

## Training Data

When upgrading to a new Mac or using setup (3) or (4) above, you can [copy SpamSieve's training data](#) from one Mac to another. This is only recommended if the two Macs will be filtering the same mail account. Macs filtering different people's mail should be trained separately for the best filtering accuracy.

Do not copy SpamSieve's files using a file synchronization program or cloud syncing utility such as Dropbox while the SpamSieve application is running. Doing so can corrupt the files.

## License Info

An individual user running SpamSieve on multiple personal Macs generally only needs to purchase one SpamSieve license. The [Purchase...](#) section of the manual has more information about the license policy.

## iCloud Rule Syncing

Multiple Macs using the same iCloud account will automatically have the same rules in Apple Mail. If you want to use the SpamSieve rule on one Mac but not the other, you should uncheck it on the Mac where you want it to be disabled. Do not delete the rule because that would (through syncing) delete it from the other Mac as well.

## POP Accounts

If you are accessing the same POP mail account from multiple Macs, you can safely run SpamSieve on all of the Macs simultaneously. Each Mac is entirely separate from the others, so you don't have to worry about any of the training issues that IMAP and Exchange accounts have. The downside is that it's more work to train each copy of SpamSieve separately.

## 3.14 iPhone Spam Filtering

### Your Mac as the Spam Filter

Due to limitations of the iOS platform, there is not currently an iPhone version of SpamSieve. However, you can use SpamSieve on your Mac to keep the spam off your iPhone, iPad, or iPod touch. The Mac has much more bandwidth and processing power, so it makes sense to do the spam filtering there, anyway. When you check for mail on your iPhone, you won't waste time or battery power downloading or processing spam messages.

### Use IMAP or Exchange to Synchronize Your Mailboxes

To use SpamSieve with your iPhone, you'll need to set both the Mac and the iPhone to connect to your mail server using either the [IMAP](#)<sup>19</sup> or [Exchange](#)<sup>20</sup> mail protocol:

- Many popular mail hosts—such as Apple's iCloud, Gmail, and Yahoo automatically uses IMAP.
- Most other modern mail hosts also offer IMAP support.
- Some hosts, such as Comcast, can enable IMAP support if you [request it](#).
- Some mail hosts only offer support for the older [POP](#)<sup>21</sup> protocol. This makes it impossible for your Mac to clean the spam off your iPhone. We recommend switching to [another provider](#).

If your mail host supports IMAP but you are not using it, you can change the settings on your Mac to connect via IMAP instead of POP. Please see the [Converting Your Apple Mail Setup to IMAP](#) section or read [Macworld's article](#)<sup>22</sup> about this.

### How IMAP/Exchange Synchronization Works

When using IMAP or Exchange, all computers and mobile devices that connect to the same mail account will share the same mailboxes. The contents of the mailboxes will be synchronized automatically. The syncing happens when you open the Mail application, not when you connect the Mac and iPhone and sync in iTunes.

### Filtering Out the Spam

You don't have to do anything extra for SpamSieve to filter the spam on your iPhone. SpamSieve is already removing the spam from your Mac's inbox, so the normal IMAP/Exchange synchronization will automatically remove the spam messages from the iPhone's inbox as well.

When your mail program is running on your Mac, it will periodically check for new mail. (See also the [Filtering Spam During Power Nap](#) section.) New messages will arrive in the inbox, and SpamSieve will move the spam messages to the spam mailbox. When the iPhone checks for new mail, the spam messages will generally already have been moved out of the inbox.

If the iPhone happens to see a new spam message before the Mac does:

- The message will appear in the inbox for a short while. When the Mac sees it, it will move it to the spam mailbox and it will disappear from the inbox on the iPhone.

---

<sup>19</sup>[http://en.wikipedia.org/wiki/Internet\\_Message\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol)

<sup>20</sup>[http://en.wikipedia.org/wiki/Microsoft\\_Exchange\\_Server](http://en.wikipedia.org/wiki/Microsoft_Exchange_Server)

<sup>21</sup>[http://en.wikipedia.org/wiki/Post\\_Office\\_Protocol](http://en.wikipedia.org/wiki/Post_Office_Protocol)

<sup>22</sup>[http://www.macworld.com/article/1165600/how\\_to\\_convert\\_a\\_pop\\_email\\_account\\_to\\_imap.html](http://www.macworld.com/article/1165600/how_to_convert_a_pop_email_account_to_imap.html)

- The iPhone supports push e-mail, which lets it see new messages instantly. If you receive a lot of spam, you may prefer to turn off the push feature. That will give the Mac a chance to filter the messages before you see them on the iPhone. You may also want to adjust your iPhone’s [notifications settings](#)<sup>23</sup> so that it doesn’t show banners or play sounds when new e-mails arrive.
- If you mark a message as read on the iPhone before the Mac sees it, the Mac will not apply its rules (such as SpamSieve) to the message.

## Checking the Spam Mailbox

With the standard setup, SpamSieve puts the spam that it catches in the **Spam** mailbox on your Mac. The spam messages are removed from the server and stored locally on the Mac. This is faster, and it means that the spam messages won’t count towards your server quota. However, this also makes it impossible to view the spam messages when you are away from your Mac.

Some users prefer to store the **Spam** mailbox on the server. This way, if SpamSieve accidentally puts a good message in the **Spam** mailbox, you can access the message on the iPhone when away from the Mac. To do this, see the [Using a Spam Mailbox on the Server](#) section.

## Training SpamSieve to Correct Mistakes

With the standard setup, you train SpamSieve directly from your Mac. If a spam message gets through to your inbox, you should not delete it from the iPhone because that would prevent you from [correcting the mistake](#).

The [Setting Up a Spam Filtering Drone](#) section describes how to set up Apple Mail for remote training. If you’ll be away from your Mac for long periods of time, you can then train SpamSieve directly from the iPhone. Correcting mistakes promptly will keep SpamSieve running at peak accuracy.

## Troubleshooting iPhone Spam Filtering

If there are spam messages in the inbox on your iPhone:

1. If the Mac hasn’t yet downloaded the spam messages at all, you may need to adjust the [Check for new messages](#) preference in Mail. Make sure that the IDLE command is enabled in Mail’s preferences for your account. With some servers, [it may help](#)<sup>24</sup> to check for new messages every minute rather than **Automatically**.
2. If the spam messages are in the inbox on your Mac, this is not an iPhone-specific problem. You should follow the regular [Why is SpamSieve not catching my spam?](#) instructions.
3. If the spam messages are in the iPhone’s inbox but in the Mac’s **Spam** mailbox, try using “pull-to-refresh” to get the iPhone to resynchronize with the server. It should then update its inbox and remove the spam messages from the inbox.
4. If the spam messages are still in the iPhone’s inbox, try logging into your mail account via Web mail.
  - If everything looks good in Web mail, there is likely a problem with your iPhone’s connection to the mail server.
  - If the spam is in the Web mail inbox but not the Mac’s, there is likely a problem with the mail program on your Mac.

<sup>23</sup><http://support.apple.com/en-us/HT201925>

<sup>24</sup><http://apple.stackexchange.com/questions/106340/mail-app-7-0-what-does-check-for-new-messages-automatically-actually-do>

### 3.14.1 Converting Your Apple Mail Setup to IMAP

This section discusses how to change your Apple Mail setup from POP to IMAP so that you can use SpamSieve for [iPhone Spam Filtering](#). A similar setup will also work with other mail programs.

1. Choose **Preferences...** from the **Mail** menu and click on **Accounts**. Your account(s) will be listed at the left of the window. If it already says **IMAP** or **iCloud** under your account, there's nothing more that you need to do.
2. If it says **POP**, you will need to disable the POP account and create a new IMAP one. Click on the POP account and make note of the contents of the **Server Settings** (if present) and **Account Information** tabs. Then click the **Remove now** button to remove from the server any messages that you've already downloaded.
3. Click the **+** button at the bottom of the window and follow the steps to create a new account. Choose **IMAP** for the account type. For the server and login, enter the information that you noted for the POP account. (*Note:* Some providers use a different incoming mail server name for IMAP.) Put "IMAP" at the end of the account's description so that you can tell this account apart from the old one.
4. You should now be able to check for mail, and Mail will be using IMAP instead of POP. There will be two sets of mailboxes (**Inbox**, **Sent**, etc.) in the main window. If desired, you can go to each of these mailboxes and Option-drag the messages from the old mailboxes to the IMAP ones. Holding down the Option key when dragging the messages will cause Mail to *copy* the messages to the IMAP server. Your original messages will remain in the POP mailboxes on your Mac in case something goes wrong.
5. Go back to Mail's **Preferences** window, click on the POP account, and uncheck **Enable this account** (in the **Account Information** tab, or the **Advanced** tab on macOS 10.11 and earlier). You will be using the new IMAP account instead, although the old POP settings, and any messages that you didn't transfer to the IMAP mailboxes, will still be available should you want to go back to the old setup.
6. On your iOS device, tap on **Settings** > **Mail**. For each of your accounts, tap on the account name. At the top of the account settings it should say **IMAP** or **Exchange**. If it says **POP**, you will need to deactivate that account on the iPhone (by sliding the switch next to the **Mail** setting) and then choose **Add Account** to re-add your account as **IMAP** or **Exchange**.

### 3.14.2 Recommended Mail Hosts

For best results with SpamSieve—and for e-mail in general—we recommend a mail host that:

#### Supports IMAP or Exchange (Not Just POP)

This will keep your mailboxes and messages synchronized across multiple devices and let you use SpamSieve on your Mac for [iPhone Spam Filtering](#). IMAP is preferred, as it is supported by more mail clients.

#### Lets You Control Its Junk Filter

You don't want the server's filter to accidentally delete good messages before you even see them. For more information, see the [How should I configure the junk filter on my mail server?](#) section.

## Is Not Your Internet Service Provider (ISP)

This way you won't be forced to change your address if you change ISPs, e.g. due to switching cable to fiber or moving to a different city.

## Can Use Your Domain Name

If your e-mail address is at a domain name that you control (rather than at the provider's domain), you won't be locked into your current host should you ever become dissatisfied with it. You'll be able to easily switch to a different host without having to change your e-mail address.

E-mail is important. If your mail provider does not offer the features that you want, we recommend switching to one that does. [Fastmail](#)<sup>25</sup>, [DreamHost](#), [Pair](#), and [Hover](#) are some inexpensive hosts that we've used and recommend. Other ones that've heard good things about are [1&1](#)<sup>26</sup>, [Cotse.Net](#)<sup>27</sup>, and [LuxSci](#)<sup>28</sup>.

# 4 Customization

## 4.1 Rule Ordering

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 AppleScript, 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.

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 Whitelisting Previous Recipients

For added safety, you can specify that addresses that you've sent mail to will never send you spam. To do this in:

### Apple Mail

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.

---

<sup>25</sup><http://www.fastmail.fm/?STKI=10293121>

<sup>26</sup><http://www.1and1.com/email-address>

<sup>27</sup><http://www.cotse.net>

<sup>28</sup><http://luxsci.com>

## Entourage

Create an outgoing rule that uses [this AppleScript](#) to add your messages' recipients to SpamSieve's whitelist.

## Mailsmith

Create a rule that uses [this AppleScript](#) to add your sent messages' recipients to SpamSieve's whitelist.

## Outlook

Create an outgoing rule that uses [this AppleScript](#) to add your messages' recipients to SpamSieve's whitelist.

## Postbox

Select **Do not mark mail as junk if the sender is in Collected Addresses** in Postbox's **Accounts** preferences.

## PowerMail

Create an outgoing filter that uses [this AppleScript](#) to add your messages' recipients to SpamSieve's whitelist.

For Apple Mail and Postbox the above settings will completely hide these messages from SpamSieve. Thus:

1. You might not want to do this if you regularly receive spam messages that are *forged* so as to appear as though they were sent from one of your previous correspondents. SpamSieve won't see the messages, so it will have no chance of catching them.
2. SpamSieve will not be able to auto-train itself with these messages. You should be sure to manually train it with some examples of these messages, so that it has seen some examples of good messages with this type of content.

## 4.3 Automatically Deleting Old Spam Messages

You can set your mail program to automatically delete old spam messages. However, if you do this, you should still review your spam messages to make sure that no good messages are deleted. Not only would you lose such messages if you don't [correct all the mistakes](#), but SpamSieve would also incorrectly learn that they are spam, leading to more mistakes in the future.

### Apple Mail

You can quickly delete all the messages in the **Spam** mailbox using the [Apple Mail - Discard Spam](#) script.

Mail also has a feature to 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.

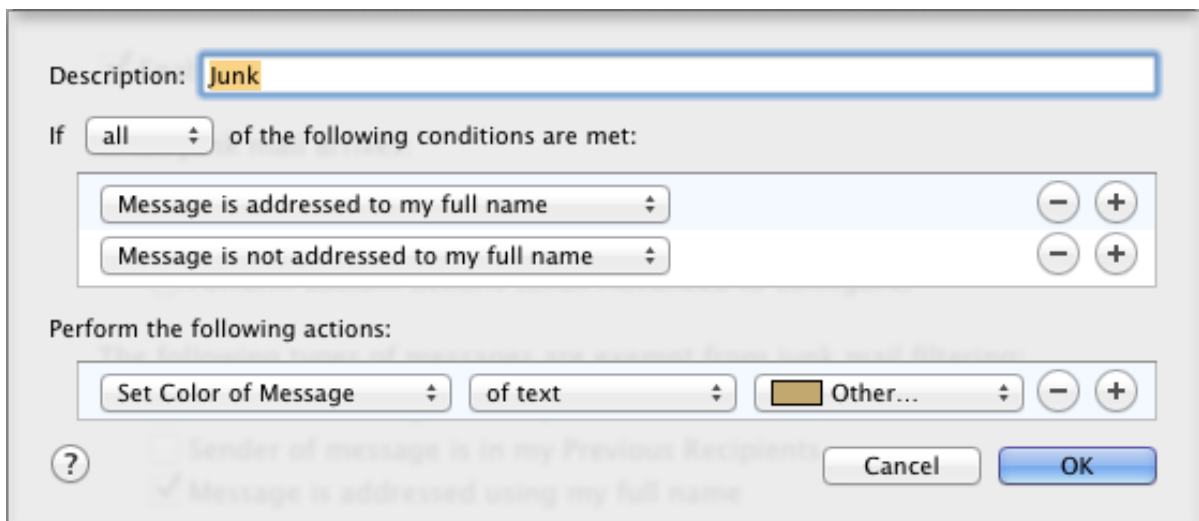
If you do this, be careful not to use the **Junk** and **Not Junk** buttons that will appear in Mail when the **Junk** mailbox is active; you should always use the **SpamSieve - Train as Good** and **SpamSieve - Train as Spam** commands instead. You can use the **Customize Toolbar...** command in Mail's **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.

1. If you want to store your spam locally (**On My Mac**) you can skip this step. If you want to store your spam on the mail server, make sure that Mail knows which mailbox is your **Junk** mailbox. To do this, create a new mailbox under your account. Select it and choose **Mailbox > Use This Mailbox For > Junk**.
2. Open Mail's **Preferences** window and click on **Junk Mail**. Make sure that **Enable junk mail filtering** is unchecked. If you can already see the special **Junk** mailbox near the top of Mail's mailbox list, you can skip to Step 3.

Otherwise, 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**. Next, 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

and set it to **If all of the following conditions are met**. Click **OK** to close the sheet. Do not make any further changes to the **Junk Mail** preferences.



3. 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.
4. Choose [SpamSieve - Change Settings](#) from Mail's **Message** menu and, when prompted, say that the name of your spam mailbox is **Junk**.
5. Go to the **Mailbox Behaviors** (or **Special Mailboxes**) tab of the Mail's **Accounts** preferences and select a time interval for **Erase junk messages** (or **Delete junk messages when**). You'll need to repeat this for each account.

*Note:* Even though you are using the **Junk** mailbox, due to a bug in Mail, the **Erase Junk Mail** command may be disabled.

## Entourage



You can set Entourage so that when it quits it will delete all the spam messages that are older than 7 days (or whichever interval you choose):

1. Choose **Tools** ▸ **Run Schedule** ▸ **Edit Schedules**.
2. Click the **New** button to create a schedule.
3. Set the name of the schedule to **Delete Old Spam**, the **When** to **On Quit**, and the **Action** to **Delete Junk Mail from Junk E-mail (On My Computer)**.
4. Click **OK** to close the dialog.

## Outlook 365

Outlook 365 does not support schedules.

## Outlook 2011

You can set Outlook so that when it quits it will delete all the spam messages that are older than 7 days (or whichever interval you choose):

1. Choose **Tools** ▸ **Run Schedule** ▸ **Edit Schedules...**
2. Click the **+** button to create a schedule.
3. Set the name of the schedule to **Delete Old Spam**, the **When** to **On Quit**, and the **Action** to **Delete Junk Mail from Junk E-mail (On My Computer)**.
4. Click **OK** to close the dialog.

## Postbox

See the **Automatically delete junk mail older than** setting in the **Accounts** preferences.

## 4.4 Setting Up a Spam Filtering Drone

As described in the [Correct All Mistakes](#) section, you need to tell SpamSieve about messages that it misclassified so that it can learn from them. Also, the sooner you correct SpamSieve the better. This presents a problem if you're going to be away from your Mac for a while, e.g. if you're on a trip and using your iPhone/iPad or Web mail. With the normal setup, you can leave SpamSieve running on your Mac at home, and it will clean the spam out of your inbox, but aside from remote-controlling your Mac there's no way to train SpamSieve.

The *drone setup* lets you run SpamSieve on one Mac and train it from other Macs, PCs, or iPhones. This setup requires Apple Mail, [MailMate](#)<sup>29</sup>, or [Microsoft Outlook 2011](#)<sup>30</sup>.

Here's an outline of how it works:

---

<sup>29</sup><http://freron.com>

<sup>30</sup><http://www.microsoft.com/mac/outlook>

- All the computers check the same IMAP, iCloud, or Exchange account.
- One Mac (the *drone*) downloads all the messages and filters them with SpamSieve. The *other computers* (your notebook Mac, your PC at work, your iPhone, etc.) are not running SpamSieve, yet they get a spam-free inbox. If you're using an iPhone, you may want to turn off push e-mail so that the phone doesn't notify you about new messages that would be put into the spam mailbox, anyway.
- If you're sitting at the drone, you can train it *normally* using the **SpamSieve - Train as Good/Spam** menu commands.
- If you're at one of the other computers, you can train it *remotely*:
  - If a spam message gets through, move it to the special **TrainSpam** mailbox to train the drone. Periodically, the drone will train the messages in this mailbox as spam and then move them to the spam mailbox.
  - If a good message ends up in the spam mailbox, move it to the special **TrainGood** mailbox to train the drone. Periodically, the drone will train the messages in this mailbox as good and then move them to the inbox.
- The Apple Mail drone checks the **Train** mailboxes whenever a new message arrives in the inbox. This can even work when your Mac is asleep, if you've enabled [Power Nap](#). The MailMate and Outlook drones check the **Train** mailboxes periodically, according to a schedule that you set. The Mac needs to be logged into your account, although you can also use other accounts via [Fast User Switching](#)<sup>31</sup>.

To set up the spam filtering drone:

1. Make sure that all the computers are set to connect to your mail account via IMAP, iCloud, or Exchange.
2. This optional step will hopefully keep SpamSieve running if there's a power failure while you're away from your drone Mac. Open System Preferences. In the **Users & Groups** pane, set Mail or Outlook as a login item for your account. Under **Login Options**, enable automatic login. In the **Energy Saver** pane, set it to **Restart automatically after a power failure**. (This option is not available on all Macs.)
3. Create two additional mailboxes in each mail account: **TrainGood** and **TrainSpam**. (If you are using Apple Mail, you don't have to do this, as the script will create the mailboxes automatically.)  
*Note:* If you don't mind (or in fact prefer) having all of your spam go to one account's **Spam** mailbox, you can instead create a single pair of training mailboxes in that account (and not create a **Spam** mailbox in each account). However, this may make it more cumbersome to move messages into the training mailboxes (e.g. from iOS or Webmail).
4. Continue following the instructions below for Apple Mail, MailMate, or Outlook.

#### 4.4.1 Setting Up an Apple Mail Drone

This section is a continuation of the [Setting Up a Spam Filtering Drone](#) instructions for people using Apple Mail.

---

<sup>31</sup>[http://support.apple.com/kb/PH4012?viewlocale=en\\_US&locale=en\\_US](http://support.apple.com/kb/PH4012?viewlocale=en_US&locale=en_US)

1. If you have a single mail account or only wish to remotely train from one account, follow the normal SpamSieve setup procedure in the [Setting Up Apple Mail](#) section, with one change: in Step 2, create the new **Spam** mailbox in your server account instead of in **On My Mac**. You're now done with this step.

*Note:* If you get an error that there is already a **Spam** mailbox in the server account, but you don't see such a mailbox, it may be that Mail is *displaying it* as the special **Junk** mailbox. Create a mailbox called **Junk** on the server and tell Mail to show it under the special **Junk** mailbox. (On macOS 10.12 and later, go to **Preferences** ▸ **Accounts** ▸ [Mailbox Behaviors](#) and choose it from the **Junk Mailbox** pop-up menu. On macOS 10.11 and earlier, select the mailbox and choose **Mailbox** ▸ **Use This Mailbox As** ▸ **Junk Mailbox**.)

If you have multiple mail accounts (and wish to remotely train from all of them):

- Create a **Spam** mailbox in each account.
- Instead of creating one **SpamSieve** rule, create one per account. The name of each rule should be **SpamSieve - Account 1** (where **Account 1** is the **Description** of your account). The conditions of the rule should say:

Account Account 1

The actions should say:

Move Message Spam [the Spam mailbox you created for this account]

Mail may ask if you want to apply the rule; click **Don't Apply**.

2. Download the [Apple Mail - Remote Training](#) script file. Open it in Script Editor (a.k.a. AppleScript Editor) and add your account name(s) at the top (as described [here](#)).
3. You can test that the script works by running it in Script Editor; it should move any messages in the **TrainGood** mailbox to the inbox and any messages in the **TrainSpam** mailbox to the **Spam** mailbox. Errors will be reported in the **All Messages** section of the Console application.
4. Go to Mail's **Preferences** window and create a new rule at the top of the list (above the **SpamSieve** rule) called **Remote Training**. (The rule's name must *not* start with **SpamSieve**.) The conditions should say:

Every Message

The actions should say:

Run AppleScript [..]Apple Mail - Remote Training.scpt

After choosing **Run AppleScript** from the pop-up menu, select the file that you created in Step 2 (using either the pop-up menu or the **Choose...** button).

Mail may ask if you want to apply the rule; click **Don't Apply**.

5. If you want manually trained spam messages to go to the **Spam** mailbox on the server rather than **On My Mac**, use the [Change Settings](#) command to tell SpamSieve that you don't want a local spam mailbox.
6. If you are using iCloud to sync your Mail rules between multiple Macs, make sure that both the **SpamSieve** and **Remote Training** rules are unchecked on all the Macs except for the drone.
7. If desired, you can set up keyboard shortcuts on any non-drone Macs for moving messages into the **Train** mailboxes. In Mail's **View** menu, choose **Show Favorites Bar**. Then drag the **TrainGood** and **TrainSpam** mailboxes to the favorites bar. There will then be keyboard shortcuts for these messages in the **Mailbox** ▸ **Move to Favorite Mailbox** submenu.

#### 4.4.2 Setting Up a MailMate Drone

This section is a continuation of the [Setting Up a Spam Filtering Drone](#) instructions for people using [MailMate](#)<sup>32</sup> 1.7.1 or later.

1. In MailMate's **Preferences** window, click on the **General** tab and make sure that next to **Experimental 2.0 Features**, the **Enable** box is checked.
2. In MailMate's **Preferences** window, click on the **Security** tab and make sure that next to **SpamSieve**, the **Enable** box is checked.
3. For each **TrainGood** mailbox, select the mailbox:
  - a) Go to the **Mailbox** menu, and choose **Edit Mailbox...**
  - b) Click on the **Rules** tab of the **TrainGood** window.
  - c) Click the **+** button at the bottom of the window.
  - d) In the **Description**, enter **Remote Good Training**.
  - e) At the bottom of the window, create two actions:
    - Set Tag: Not Junk
    - Move to Mailbox: Inbox
4. For each **TrainSpam** mailbox, select the mailbox:
  - a) Go to the **Mailbox** menu, and choose **Edit Mailbox...**
  - b) Click on the **Rules** tab of the **TrainSpam** window.
  - c) Click the **+** button at the bottom of the window.
  - d) In the **Description**, enter **Remote Spam Training**.
  - e) At the bottom of the window, create two actions:
    - Set Tag: Junk
    - Move to Mailbox: Junk
5. MailMate will check the **Train** mailboxes according to the **Synchronization Schedule** in the **Mailbox** menu.

#### 4.4.3 Setting Up an Outlook Drone

This section is a continuation of the [Setting Up a Spam Filtering Drone](#) instructions for people using [Microsoft Outlook 2011](#)<sup>33</sup>. Outlook 365 currently does not work with the drone setup because it does not support schedules.

1. Make sure that each of your accounts has its own **Junk E-mail** mailbox. This can be configured by going to the **Accounts** section of Outlook's preferences and clicking on **Advanced...** and then **Folders**.

---

<sup>32</sup><http://freron.com>

<sup>33</sup><http://www.microsoft.com/mac/outlook>

2. If you have a single mail account, follow the normal SpamSieve setup procedure in the [Setting Up Outlook 2011](#) section. When choosing the folder in the **SpamSieve - Move Messages** rule, be sure to choose the **Junk E-mail** folder on the server (not **On My Computer**). You're now done with this step.

If you have multiple accounts, create *two* **SpamSieve - Move Messages** rules per account. The name of the first rule should be **SpamSieve - Move Junk Messages - Account 1** (where **Account 1** is the name of your account. It should say:

If all conditions are met:

- Folder Is INBOX (Account 1)
- Category Is Junk

Do the following:

Move Message Junk E-mail (Account 1)

The name of the second rule should be **SpamSieve - Move Uncertain Junk Messages - Account 1**. It should say:

If all conditions are met:

- Folder Is INBOX (Account 1)
- Category Is Uncertain Junk

Do the following:

Move Message Junk E-mail (Account 1)

3. Download the [Outlook - Remote Training](#) script file. Open it in Script Editor and add your account name(s) at the top.
4. In Outlook, choose **Tools** ▸ **Run Schedule** ▸ **Edit Schedules...** Click the + button and create a schedule called **Remote Training**. The **When** should be **Repeating Schedule** with a duration of your choice. The **Action** should be **Rule AppleScript**. Click the **Script...** button and choose the `Outlook - Remote Training.scpt` file from Step 4.

## 4.5 Customizing Using AppleScript

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](#) is available.

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](mailto:spamsieve@c-command.com)<sup>34</sup> for assistance.

## 4.6 Apple Mail Customization

The following customizations are optional but recommended:

---

<sup>34</sup><mailto:spamsieve@c-command.com>

## Notifications

Choose **Mail** ▸ **Preferences...** and click on **General**. Change the **New messages sound** to **None** so that Apple Mail does not play a sound when spam messages arrive. Change **New message notifications** to **Inbox Only** (or to a custom smart mailbox that excludes your **Spam** mailbox). This will prevent Mail from notifying you when you receive new spam messages. SpamSieve will **notify** you only when you receive new good messages.

## Account Aliases

Tell Mail and SpamSieve about your account aliases, as described in the [Why do good messages move to the wrong inbox when trained in Apple Mail?](#) section.

## Unread Smart Mailbox

If you have an “Unread” smart mailbox, please see the [Why do I see spam messages in my “Unread” smart mailbox in Apple Mail?](#) section for how to adjust it.

## Sleep

Sometimes Mail rules will **not move messages** that were processed immediately after the Mac woke from sleep. If this happens, you will end up with spam messages that are marked as spam but not moved from the inbox to the **Spam** mailbox. You can work around this problem by quitting Mail before sleeping your Mac or by changing the **Energy Saver** settings so that your Mac will not go to sleep automatically.

Additional customizations are described below:

### 4.6.1 Faster Apple Mail Training

#### macOS 10.10 and Later

The issue described below for macOS 10.9 rarely affects later versions, but there are still some cases where Mail is slow at moving messages when you train them as spam or as good. To speed up the training, you can enable the workarounds by using these special [esoteric preferences](#) links:

#### AppleMailTrainSpamGUIScriptingYosemite

Click [this link](#)<sup>35</sup> to enable the workaround for making **SpamSieve - Train as Spam** faster. The first time you try to train a message, SpamSieve will ask you to give it accessibility privileges. Then it will ask you to add your **Spam** mailbox as a favorite in Mail. Thereafter, it will move the trained messages via GUI scripting. If an error occurs, SpamSieve will move the message via the more reliable but slower method. Click [this link](#)<sup>36</sup> to disable the workaround.

#### AppleMailTrainGoodGUIScriptingYosemite

Click [this link](#)<sup>37</sup> to enable the workaround for making **SpamSieve - Train as Good** faster. SpamSieve will ask you to add your inbox as a favorite in Mail. Trained messages will now move to the inbox that you added in the favorites bar, whereas without the workaround SpamSieve will **try to find** the appropriate account's inbox. Click [this link](#)<sup>38</sup> to disable the workaround.

---

<sup>35</sup>`x-spamsieve://default?k=AppleMailTrainSpamGUIScriptingYosemite&v=YES`

<sup>36</sup>`x-spamsieve://default?k=AppleMailTrainSpamGUIScriptingYosemite&v=NO`

<sup>37</sup>`x-spamsieve://default?k=AppleMailTrainGoodGUIScriptingYosemite&v=YES`

<sup>38</sup>`x-spamsieve://default?k=AppleMailTrainGoodGUIScriptingYosemite&v=NO`

## AppleMailChangeJunkStatus

Another potential slowdown is that Mail can hang when it's telling *its own* junk filter that the message is junk. Normally, SpamSieve tries to keep Mail in the loop so that when you train a message as spam, SpamSieve tells Mail that the message is junk. However, in rare circumstances a bug in Mail or a slow mail server can cause Mail to freeze when setting the message as junk. You can tell SpamSieve *not* to tell Mail's filter that the message is junk by clicking [this link](#)<sup>39</sup>. Or, click [this link](#)<sup>40</sup> to go back to the default behavior.

## macOS 10.9

There is a known issue where Apple Mail on macOS 10.9 is slower at moving messages via AppleScript. This can cause delays/freezes of up to 10 seconds when using the **SpamSieve - Train as Spam** and **SpamSieve - Train as Good** commands. SpamSieve includes workarounds to move messages faster by using GUI scripting instead of regular AppleScript.

You can enable one or both workarounds by using these special [esoteric preferences](#) links:

### AppleMailTrainSpamGUIScripting

Click [this link](#)<sup>41</sup> to enable the workaround for making **SpamSieve - Train as Spam** faster. The first time you try to train a message, SpamSieve will ask you to give it accessibility privileges. Then it will ask you to add your **Spam** mailbox as a favorite in Mail. Thereafter, it will move the trained messages via GUI scripting. If an error occurs, SpamSieve will move the message via the more reliable but slower method. Click [this link](#)<sup>42</sup> to disable the workaround.

### AppleMailTrainGoodGUIScripting

Click [this link](#)<sup>43</sup> to enable the workaround for making **SpamSieve - Train as Good** faster. SpamSieve it will ask you to add your inbox as a favorite in Mail. Trained messages will now move to the inbox that you added in the favorites bar, whereas without the workaround SpamSieve will [try to find](#) the appropriate account's inbox. Click [this link](#)<sup>44</sup> to disable the workaround.

## Accessibility Troubleshooting

- Due to an OS bug, **SpamSieveHelper** may not automatically appear in the list of **Accessibility** applications. To add it manually, you can:
  1. If necessary, click the lock button next to **Click the lock to make changes**.
  2. Command-click on the SpamSieve icon in the Dock to reveal the SpamSieve application file in the Finder.
  3. Control-click on the SpamSieve application file and choose **Show Package Contents**.
  4. Open the **Contents** folder and then the MacOS folder.
  5. Drag and drop the SpamSieveHelper file into the **Allow the apps below to control your computer** list in System Preferences.

---

<sup>39</sup>`x-spamsieve://default?k=AppleMailChangeJunkStatus&v=NO`

<sup>40</sup>`x-spamsieve://default?k=AppleMailChangeJunkStatus&v=YES`

<sup>41</sup>`x-spamsieve://default?k=AppleMailTrainSpamGUIScripting&v=YES`

<sup>42</sup>`x-spamsieve://default?k=AppleMailTrainSpamGUIScripting&v=NO`

<sup>43</sup>`x-spamsieve://default?k=AppleMailTrainGoodGUIScripting&v=YES`

<sup>44</sup>`x-spamsieve://default?k=AppleMailTrainGoodGUIScripting&v=NO`

- In rare cases, SpamSieve may report that **SpamSieveHelper** is not checked in the **Accessibility** preferences, even though it actually is. This typically means that macOS’s privacy database has been corrupted. You can reset the database by entering this command in Terminal:

```
tccutil reset Accessibility
```

## The Drone Setup

Aside from the GUI Scripting workaround (above), you can also speed up training by following the [Setting Up a Spam Filtering Drone](#) instructions. Instead of using the **Message** menu commands to train messages, you would move the messages into the special **TrainGood** and **TrainSpam** mailboxes.

### 4.6.2 Change Settings (Apple Mail)

You can choose **SpamSieve - Change Settings** from Mail’s **Message** menu to customize SpamSieve’s behavior in 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)?
- 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)?

### 4.6.3 Apple Mail Keyboard Shortcuts

The keyboard shortcut for the **SpamSieve - Train as Spam** command is Command-Control-S. The keyboard shortcut for the **SpamSieve - Train as Good** command is Command-Control-G. You can change the keyboard shortcuts:

1. Open **System Preferences**.
2. Click on the **Keyboard** icon.
3. Click on the **Shortcuts** (or **Keyboard Shortcuts** on older versions of macOS) tab.
4. Select **App Shortcuts** (or **Application Shortcuts** on older versions of macOS).
5. Click the + button.



6. For **Application**, select **Mail**.
7. For the **Menu Title**, enter **SpamSieve - Train as Spam** (or the localized title of the menu item if you are running your Mac in a different language).
8. Click in the box next to **Keyboard Shortcut** and enter your desired shortcut.
9. Click the **Add** button.

#### 4.6.4 Spam Message Colors in Apple Mail

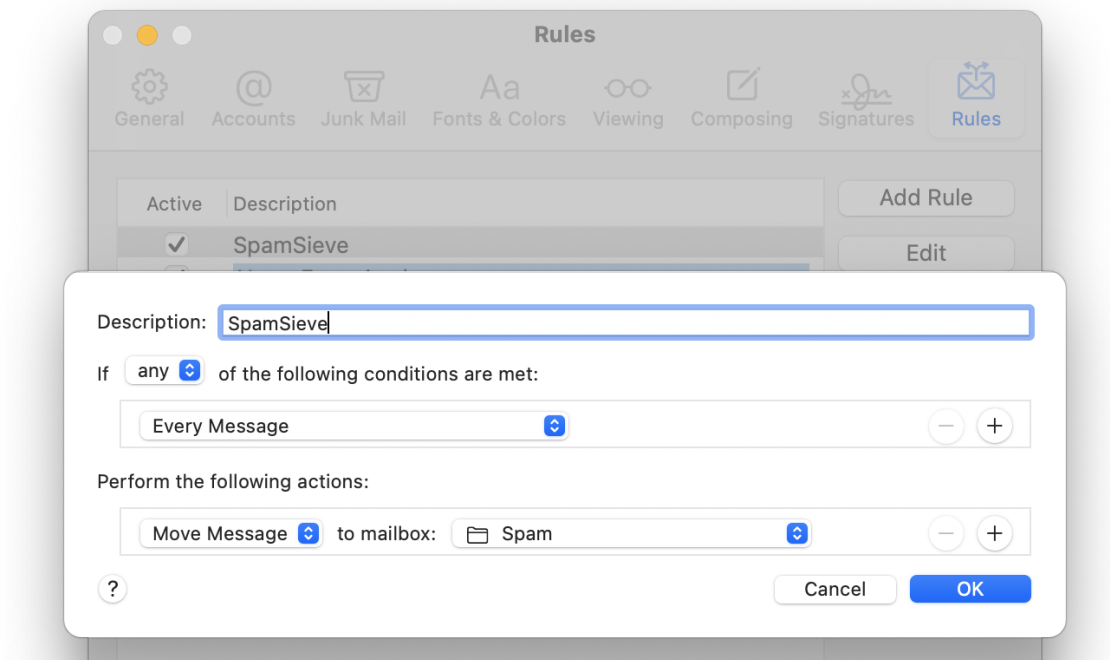
##### Using Background Colors to Show Spam Levels

SpamSieve sets the colors of spam messages to reflect how spammy it thinks they are. The order, from most to least spammy, is: Blue, Gray, Purple, Red, Orange, or Yellow. Good messages are left uncolored. Thus, if you are skimming the **Spam** mailbox for false positives, pay the most attention to the yellow and orange messages. The [SpamSieve - Change Settings](#) command lets you enable or disable spam message coloring.

Spam messages caught by a [server junk filter](#) are not processed by SpamSieve and, thus, not colored.

##### Using a [Score] Rule to Filter Spam Messages By Color

The [Setting Up Apple Mail](#) section of the manual shows how to create a single rule in Mail that puts all the spam messages in a single **Spam** mailbox. You can also use multiple rules in Mail to file messages into different mailboxes (or otherwise process them differently) based on how spammy they are. The normal SpamSieve rule looks like this:



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 **Every Message**. 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.

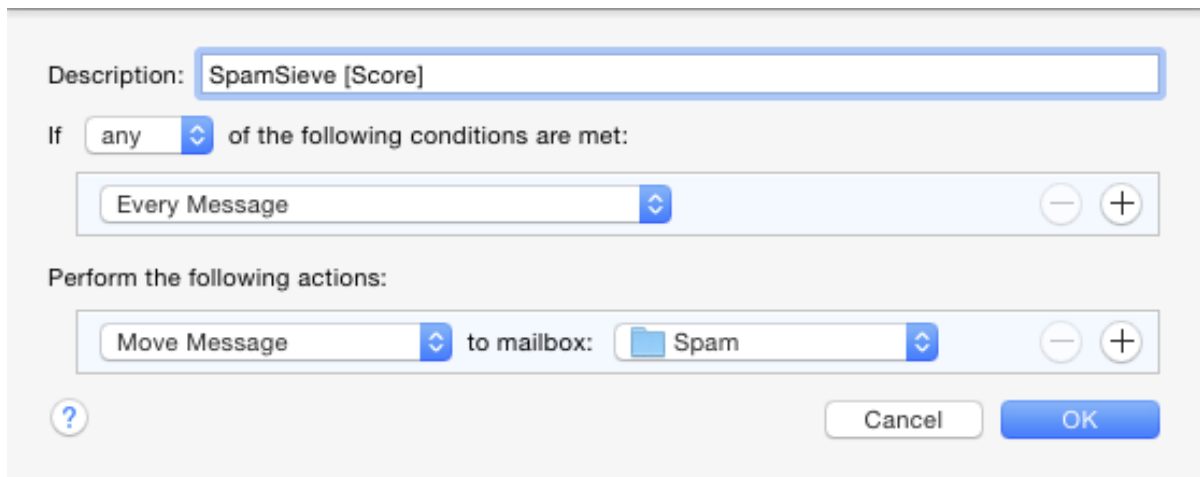
Below the **[Score]** rule, you can create one or more rules that process messages based on their color:

- Each of these rules should have a name that starts with **SpamSieve**, followed by one or more color names in square brackets. 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]**). You can include additional descriptive text after the brackets to remind you of what the rule does.
- The rule conditions should be **Every Message**.
- As a shorthand for listing *all* of the colors, you can simply write **[Spam]**.
- To match non-spam messages you can write **[White]**. Additionally, if you have rules to process every color and those rules' actions either move the messages or stop rule processing, any subsequent rules will automatically apply only to the non-spam messages.

### Example 1: Blocklisted Messages in Trash

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) / Every Message / Move Message to mailbox Spam



The screenshot shows a rule configuration window for SpamSieve. The 'Description' field contains 'SpamSieve [Score]'. Under the 'If' section, a dropdown menu shows 'any' and a button indicates 'of the following conditions are met:'. Below this, a list of conditions contains 'Every Message'. The 'Perform the following actions:' section shows a list of actions with 'Move Message' selected, followed by 'to mailbox:' and a dropdown menu showing 'Spam'. At the bottom, there are 'Cancel' and 'OK' buttons, and a help icon (?) on the left.

2. SpamSieve [Blue] (move very spammy messages to the trash) / Every Message / Move Message to mailbox Trash

Description: SpamSieve [Blue]

If any of the following conditions are met:

- Every Message

Perform the following actions:

- Move Message to mailbox: Trash

Buttons: ? (help), Cancel, OK

3. SpamSieve [Spam] (move the remaining spam messages) / Every Message / Move Message to mailbox Spam

Description: SpamSieve [Spam]

If any of the following conditions are met:

- Every Message

Perform the following actions:

- Move Message to mailbox: Spam

Buttons: ? (help), Cancel, OK

## Example 2: Per-Color Spam Mailboxes

To put each color of spam in a separate mailbox, you would need seven rules:

1. SpamSieve [Score] (calculates the spam score/color) / Every Message / Move Message to mailbox Spam
2. SpamSieve [Blue] (messages with scores from 99 to 100) / Every Message / Move Message to mailbox Spam99
3. SpamSieve [Gray] (messages with scores from 95 to 98) / Every Message / Move Message to mailbox Spam95
4. SpamSieve [Purple] (messages with scores from 88 to 94) / Every Message / Move Message to mailbox Spam88

5. SpamSieve [Red] (messages with scores from 81 to 87) / Every Message / Move Message to mailbox Spam81
6. SpamSieve [Orange] (messages with scores from 75 to 80) / Every Message / Move Message to mailbox Spam75
7. SpamSieve [Yellow] (messages with scores from 50 to 74) / Every Message / Move Message to mailbox Spam50

The unnumbered **Spam** mailbox will hold the messages that you manually train as spam. If desired, you can drag the other mailboxes inside the **Spam** mailbox.

### Example 3: Sorting Messages By Spamminess

You can sort the messages by spamminess. Apple Mail in macOS 10.7 and later cannot sort messages by color, but it can sort them by flags. Thus, you can set up rules like this:

1. SpamSieve [Score] (calculates the spam score/color) / Every Message / Move Message to mailbox Spam
2. SpamSieve [Blue] (messages with scores from 99 to 100) / Every Message / Mark as Flagged Gray / Move Message to mailbox Spam
3. SpamSieve [Gray] (messages with scores from 95 to 98) / Every Message / Mark as Flagged Purple / Move Message to mailbox Spam
4. SpamSieve [Purple] (messages with scores from 88 to 94) / Every Message / Mark as Flagged Blue / Move Message to mailbox Spam
5. SpamSieve [Red] (messages with scores from 81 to 87) / Every Message / Mark as Flagged Green / Move Message to mailbox Spam
6. SpamSieve [Orange] (messages with scores from 75 to 80) / Every Message / Mark as Flagged Yellow / Move Message to mailbox Spam
7. SpamSieve [Yellow] (messages with scores from 50 to 74) / Every Message / Mark as Flagged Orange / Move Message to mailbox Spam

and then choose **View** ▸ **Sort By** ▸ **Flags**. (The flag colors are chosen so that the messages will sort in order of spamminess; this is why they do not match the message colors.) When using this rule, you should set the **AppleMailTrainGoodClearFlags** option in the [Esoteric Preferences](#) to have SpamSieve clear the flags when training a message as good.

Currently, there is a bug (Radar 21468415) in macOS 10.11 where the feature to sort by flags does not work.

### 4.6.5 Changing the Name of the Spam Mailbox

You can change which mailboxes SpamSieve uses to store your spam.

1. Change the mailbox where SpamSieve moves incoming spam messages:

- If your preferred mailbox does not exist yet, 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.
  - If your preferred mailbox already exists, open the **SpamSieve** rule in Mail's preferences and choose that mailbox from the pop-up menu.
2. Change the mailbox for manually trained spam messages, i.e. when you use the **SpamSieve - Train as Spam** command:
    - a) Choose [SpamSieve - Change Settings](#) from Mail's **Message** menu.
    - b) When prompted, enter the new mailbox name. This does not have to be the same name as in Step 1. If a top-level mailbox with this name does not exist, SpamSieve will create one when you train a message as spam.
  3. If you are using the [Apple Mail - Remote Training](#), [Apple Mail - SaneBox](#), or [Apple Mail - Server Junk Mailbox](#) script you may want to modify the top of the script to tell it to use your new mailbox name.

### Example 1: Spam Mailbox at the Top of the List

You can put a space at the beginning of the mailbox name so that it sorts to the top of the list. Mailboxes can also be dragged and dropped to reorder them in Apple Mail, although this does not affect the order on other devices the way renaming does.

### Example 2: Putting Spam in the Trash

Some people like to enter **Deleted Messages** in Step 2 so that messages trained as spam are moved directly to the trash. This is safe because you know for sure that those messages are spam. Incoming spam messages can still go to the **Spam** mailbox selected in Step 1 so that you can review them.

It is also possible to select the trash in Step 1 so that incoming spam messages go directly to the trash. Some people like this because Mail has a setting (**Preferences** ▸ **Accounts** ▸ **Mailbox Behaviors**) to automatically delete old messages from the trash. However, if you do this, make sure that you periodically check to make sure there are no good messages in the trash. Not only would you lose such messages if you don't [correct all the mistakes](#), but SpamSieve would also incorrectly learn that they are spam, leading to more mistakes in the future.

### Example 3: Putting Spam in the Junk Mailbox

Please see the [Automatically Deleting Old Spam Messages](#) section.

## 4.6.6 Using a Spam Mailbox on the Server

[Normally](#) the **Spam** mailbox is kept on your Mac, as this is faster and doesn't fill up your server account with spam. If you prefer to keep the spam on your mail server (so that it's available on [all your devices](#)), you can:

1. Go to Mail's **Mailbox** menu and choose **New Mailbox...** Use the **Location** pop-up menu to choose your IMAP or Exchange server, and enter **Spam** in the **Name** field. Click **OK**.

If you are using Gmail, there is already a **Spam** mailbox on the server. You can use this one instead of creating a new mailbox. If you are using macOS 10.11 or earlier, you will need to enter [Gmail] as the **IMAP Path Prefix** in the **Advanced** section of Mail's **Accounts** preferences. This will make the **Spam** mailbox appear at the top level of the account in Mail's mailbox list.

2. Open Mail's preferences and find the **SpamSieve** rule. Choose the server mailbox that you want to use.

You can optionally use a separate mailbox for each account. To do this, create one **Spam** mailbox per account, and then one rule per account, as described in [Separate Spam Mailboxes for Each Account](#).

3. In Mail's **Message** menu, choose **SpamSieve - Change Settings**. Enter the name of the mailbox created in Step 1. When it asks you, "Should messages marked using "Train as Spam" be stored in a local spam mailbox (rather than on the server)?" click **No**.
4. If you had created a **Spam** mailbox under **On My Mac** as described in the [Setting Up Apple Mail](#) section, it is now longer needed, and you can delete it.
5. Now both the incoming and trained spam messages will go to the **Spam** mailbox on the server. If you find a good message in the **Spam** mailbox and you're at your Mac, use the **SpamSieve - Train as Good** command as normal. If you're using an iPhone, iPad, Webmail, or a different Mac:
  - If you are using the regular SpamSieve setup, do not move the message out of the **Spam** mailbox. Instead, when you get back to your Mac, select the message and choose **SpamSieve - Train as Good**.
  - If you are using the [drone setup](#), you can move the message to the **TrainGood** mailbox. The Mac will automatically train it as good and move it to your inbox.

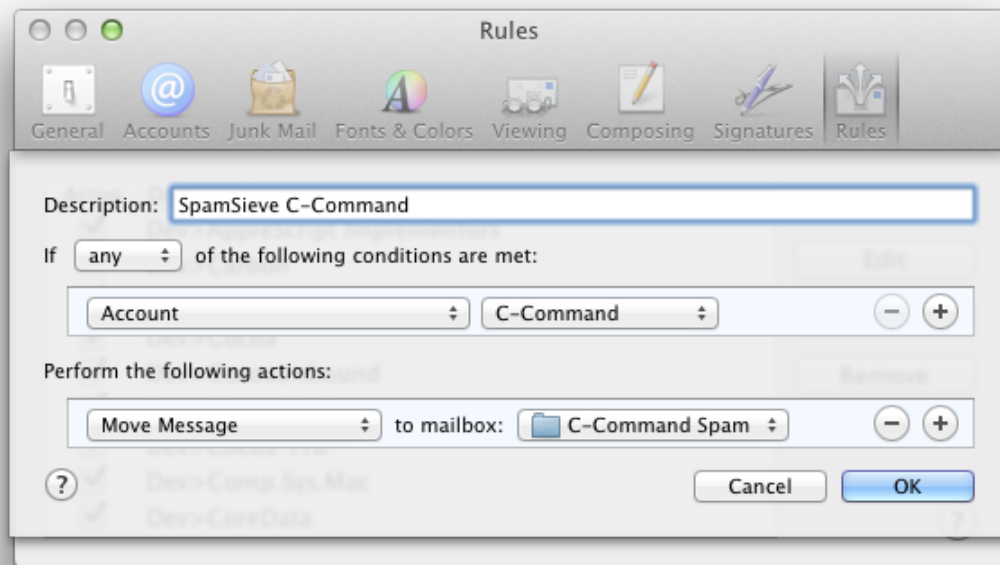
#### 4.6.7 Marking Incoming Spam Messages

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. When all the messages in a mailbox are marked as read, Apple Mail will stop showing a number next to the mailbox.

Do not add an action that changes the color of the message, as it will not do what you expect.

#### 4.6.8 Separate Spam Mailboxes for Each Account

SpamSieve normally 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.

#### 4.6.9 Only Filtering Certain Accounts

SpamSieve normally filters all of the accounts set up in Apple Mail. If you want to exclude certain accounts from filtering, you can edit the **SpamSieve** rule to list only the accounts that you *do* want filtered:

Description:

If  of the following conditions are met:

|  |                                       |                                  |                                  |
|--|---------------------------------------|----------------------------------|----------------------------------|
| <input type="button" value="Account"/> | <input type="button" value="iCloud"/> | <input type="button" value="−"/> | <input type="button" value="+"/> |
| <input type="button" value="Account"/> | <input type="button" value="Gmail"/>  | <input type="button" value="−"/> | <input type="button" value="+"/> |

Perform the following actions:

|   |   |                                  |                                  |
|---|---|----------------------------------|----------------------------------|
| <input type="button" value="Move Message"/> | to mailbox: <input type="button" value="Spam"/> | <input type="button" value="−"/> | <input type="button" value="+"/> |
|---|---|----------------------------------|----------------------------------|

#### 4.6.10 Redirecting Good Messages to Another Account

When traveling, especially with a mobile device, you might want to avoid downloading spam messages from the server. If your server and mobile device support IMAP or Exchange, you can do this by following the instructions in the [Using a Spam Mailbox on the Server](#) section.

If your mobile device only supports POP, 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.

#### 4.6.11 Consolidating Spam From Multiple Filters

As described in the [How should I configure the junk filter on my mail server?](#) section, we generally recommend turning off other spam/junk filters and only using SpamSieve. If you choose not to do this you may end up in a situation where server filters are putting spam messages in one or more **Junk** mailboxes, while SpamSieve puts messages in the **Spam** mailbox. This section describes different strategies for coping with multiple **Junk/Spam** mailboxes in Apple Mail. This is especially useful if you are using a mail host, [such as iCloud](#), whose junk filter cannot be turned off. You should pick just one of the lettered strategies below.

##### A. Have Separate Mailboxes for Each Spam/Junk Filter

Some users like having separate **Junk** and **Spam** mailboxes. If this is what you want, just be sure to check both locations for false positives, so that no good messages get stuck there. Only good messages in the **Spam** mailbox need to be trained as good because good messages in the **Junk** mailbox are not SpamSieve mistakes.



## B. Use a Smart Mailbox to Show All the Spam in One Place

You can create a smart mailbox to show the contents of all the mailboxes in one place. For example, it might look like this:

Contains messages that match *any* of the following conditions:

- Message is in mailbox **Junk**
- Message is in mailbox **Spam**

You will still have the separate (actual) mailboxes, but you will be able to review all of your spam at once (in the smart mailbox).

## C. Tell SpamSieve to Use the Junk Mailbox

You may not be able to change where your server filters put spam messages, but you can change what SpamSieve does. You can tell it to put the spam in Mail's special **Junk** mailbox, which the server junk filters are probably already using. The messages will still be stored under their respective accounts, but there will be less visual clutter.

1. For each account, find the mailbox that the server junk filter is using and tell Mail to show it under the special **Junk** mailbox.
  - On macOS 10.12 and later, go to **Preferences** ▸ **Accounts** ▸ **Mailbox Behaviors** and choose it from the **Junk Mailbox** pop-up menu.
  - On macOS 10.11 and earlier, select the mailbox and choose **Mailbox** ▸ **Use This Mailbox As** ▸ **Junk Mailbox**.
2. Change the **SpamSieve** rule to move messages to the special **Junk** mailbox rather than the **Spam** mailbox.
3. Choose [SpamSieve - Change Settings](#) from Mail's **Message** menu and, when prompted, enter **Junk** as the name of the mailbox for trained spam messages.
4. Delete any **Spam/Junk** mailboxes that are no longer in use.

With this setup, the only way to tell whether SpamSieve or a server filter was what classified a message as spam is to [look in SpamSieve's log](#).

## D. Manually Re-filter the Junk Mailbox to Rescue Good Messages

The above methods put all your spam in one place, but they have the disadvantage that the server filter may mistakenly put good messages in the **Junk** mailbox. To consolidate your spam and have SpamSieve save you from this type of server mistake:

1. Periodically, select all the messages in the **Junk** mailbox.
2. Go to Mail's **Message** menu, and choose **Apply Rules**. SpamSieve will move the messages that it thinks are spam to the **Spam** mailbox.
3. Any messages left in the **Junk** mailbox are probably good. You can then move them to your inbox. (If there are any spam messages left, you should train them as spam.)

## E. Automatically Re-filter the Junk Mailbox to Rescue Good Messages

You can use the [Apple Mail - Server Junk Mailbox](#) script to automate this sort of re-filtering. Whenever the script runs, it will tell SpamSieve to examine the messages in the **Junk** mailbox, moving the spam messages to the **Spam** mailbox and the good messages to the inbox. You can optionally set it to mark the spam messages as read.

### 4.6.12 Filtering Spam During Power Nap

In order for SpamSieve to filter your mail quickly, your Mac needs to be awake with the mail program running. Otherwise, there will be delays for [iPhone spam filtering](#) and the [drone setup](#). In the **Energy Saver** pane in **System Preferences**, we recommend setting **Computer sleep** to **Never** (when on **Power Adapter**). You can still save energy by setting the Mac's display and hard disks to sleep.

Newer Macs and versions of the OS support a feature called [Power Nap](#)<sup>45</sup>, which can let SpamSieve run *once per hour* even when your Mac is asleep.

- Power Nap requires macOS 10.8 or a later for notebooks and macOS 10.9 or later for desktops. The supported Macs are listed [here](#)<sup>46</sup>.
- You need to enable Power Nap in the **Energy Saver** pane in **System Preferences**. Notebooks have separate settings for enabling Power Nap when on battery or AC power.
- In order for Power Nap to work, the Mac needs to be connected to the Internet, and Apple Mail needs to be running before you put the Mac to sleep.
- The Mac will suspend Power Nap operations if your Mac is likely to overheat.
- When everything is set up as described above, Mail will check for new messages and filter them through SpamSieve once per hour.

### 4.6.13 Keeping Spam Messages Out of Gmail's Archive

The [standard Apple Mail setup](#) has you configure Mail to move all spams that SpamSieve catches to a local **Spam** mailbox under **On My Mac**. This is to prevent the spam from filling up your mail account and also so that all your spam is consolidated into a single mailbox for easy review and deletion.

With the default Gmail settings, when a message is moved to a local mailbox, Gmail archives the message. Combined with the above, this means that the spam messages that SpamSieve catches will go into your Gmail archive (**All Mail**). There are two ways to prevent this:

- Tell Gmail not to archive messages that are deleted via IMAP (which includes messages moved to local mailboxes on your Mac):
  1. Click the gear at the top right, choose **Settings**, then click on **Forwarding and POP/IMAP**.

---

<sup>45</sup><http://support.apple.com/kb/HT5394>

<sup>46</sup><http://support.apple.com/kb/HT5394>

2. Select **Auto-Expunge off** and **Immediately delete the message forever**.

**IMAP Access:**

(access Gmail from other clients using IMAP)

[Learn more](#)

**Status: IMAP is enabled**

- ☒ Enable IMAP
- ☐ Disable IMAP

**When I mark a message in IMAP as deleted:**

- ☐ Auto-Expunge on - Immediately update the server. (default)
- ☒ Auto-Expunge off - Wait for the client to update the server.

**When a message is marked as deleted and expunged from the last visible IMAP folder:**

- ☐ Archive the message (default)
- ☐ Move the message to the Trash
- ☒ Immediately delete the message forever

- [Use a Spam mailbox on the server](#). For example, have SpamSieve put the spam it catches into the special **Junk** mailbox on the Gmail server.

#### 4.6.14 Hiding Special Gmail Mailboxes From IMAP

Gmail has some special mailboxes that most users do not want to appear in Apple Mail. This is because these mailboxes contain duplicate copies of messages that are already in your other mailboxes. Additionally, the contents of these mailboxes are not filtered by SpamSieve or other Mail rules. When using Gmail, it is recommended that you hide these mailboxes from IMAP:

1. In Gmail, click on the gear menu at the top right and select **Settings**.
2. Click on **Labels** (which is next to **General** at the top of the screen).
3. In the **System labels** section:
  - a) Uncheck **Show in IMAP** on the line for **Starred**.
  - b) Uncheck **Show in IMAP** on the line for **Important**.
  - c) Uncheck **Show in IMAP** on the line for **All Mail**.

#### 4.6.15 Apple Mail Script Rule

Normally, SpamSieve uses a [plug-in](#) and a [special rule](#) to move spam messages to the spam mailbox. In some circumstances, you may prefer to use an alternate setup:

- There's a bug in macOS 10.15, affecting a small number of customers, which can prevent messages caught by the normal **SpamSieve** rule from moving to the spam mailbox, leaving them [colored in the inbox](#).

- You may be using a pre-release version of macOS, which is [not yet supported](#) by the SpamSieve plug-in.
- You may prefer not to install the SpamSieve plug-in, e.g. to troubleshoot a [Mail crash](#) or a [potential conflict](#) with another Mail plug-in.

In such situations, you can uncheck the **SpamSieve** rule in Mail’s preferences (or skip creating it in the first place) and instead set up a script rule:

1. Choose **Preferences...** from the **Mail** menu and click the **Rules** button in the toolbar.
2. Click the **Add Rule** button.
3. Change the description to **Move If SpamSieve Spam**.
4. Change the **From** (or **Any Recipient**, prior to macOS 10.12) pop-up menu to say **Every Message**. (**Every Message** is near the bottom of the menu.)
5. Change the **Move Message** pop-up menu to say **Run AppleScript**.
6. Next to **Run AppleScript**, change the **No Script Selected** pop-up menu to say **Move If SpamSieve Spam**. (The script should be pre-installed when you install SpamSieve’s plug-in. It’s also available for download [here](#).)
7. Now click **OK** to close the rule and save your changes. Mail may ask if you want to apply the rule; click **Don’t Apply**. (If you were to click **Apply** now, or in the future when editing a rule, that would filter all of the currently displayed old messages through SpamSieve, and you would be obliged to correct any mistakes.)

Disadvantages of the **Move If SpamSieve Spam** script rule compared with the regular **SpamSieve** rule:

- The script rule is slower.
- With the **SpamSieve** rule, Mail will not apply subsequent rules if the message is spam. With a rule that runs the script, Mail will keep applying the rest of the rules.

#### 4.6.16 Processing Messages Before SpamSieve

Sometimes you may wish to prevent certain messages from being examined by SpamSieve. You can do this by making an Apple Mail rule above the **SpamSieve** rule that moves the messages to a different mailbox or deletes them.

1. You may receive messages that are unwanted but not spam, for example if someone you know sends you a certain type of annoying message. You don’t want to see these, but it’s not appropriate to train SpamSieve that they’re spam because they’re from a legitimate sender.  
*Solution:* Make a Mail rule above the **SpamSieve** rule that moves these messages to the trash.
2. The messages may be ambiguously spam. For example, you may run a Web site that sends you an e-mail every time someone fills out a form. The messages themselves are not spam; they are being sent by your own server. But some of the content in the e-mails may be spammy, depending on

what the users (or robots) filled into the form. You want to receive all these messages to review them, but you don't want to train SpamSieve that all the user-generated text is good.

*Solution:* Make a Mail rule above the **SpamSieve** rule that moves these messages to a separate mailbox.

3. You may have a way of identifying certain messages as definitely spam, and you want Mail to delete them so that you don't have to see them in your **Spam** mailbox.

*Solution:* Make a Mail rule above the **SpamSieve** rule that deletes the messages.

(If you merely want to move the more spammy messages to the trash, see the [Spam Message Colors in Apple Mail](#) section.)

Here's an example of how to create a rule for #3:

1. Choose **Preferences...** from the **Mail** menu and click the **Rules** button in the toolbar.
2. Click the **Add Rule** button.
3. Change the description to **Delete Spam**.
4. Say that you want to block messages from certain e-mail addresses. The rule conditions already say **From contains**. Enter the first address to block in the text field to the right of **contains**.
5. For each additional address, click the **+** button and enter the address in the new **From contains** condition.
6. At the bottom of the sheet, change **Move Message** to say **Delete Message**. The rule should now look like:

The screenshot shows the 'Add Rule' dialog box in Apple Mail. The 'Description' field is set to 'Delete Spam'. The 'If' section is configured with the condition 'any of the following conditions are met:'. There are two conditions listed: 'From' contains 'a@b.com' and 'From' contains 'c@d.com'. The 'Perform the following actions' section is set to 'Delete Message'. The 'OK' button is highlighted in blue.

7. Now click **OK** to close the rule and save your changes. Mail may ask if you want to apply the rule; click **Don't Apply**.
8. Drag the **Delete Spam** rule to the top of the list, above the **SpamSieve** rule.

## 4.7 Outlook Customization

The following customizations are optional but recommended:

- Choose **Outlook** ▸ **Preferences...** and click on **Notifications & Sounds**. Turn off the alerts and sounds for 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...** Select your account and click the **Advanced...** button. Make sure that **Download headers only** is unchecked.

The [Outlook Filter Mailboxes script page](#) describes some additional advanced features such as checking for new messages more frequently and enabling debug logging.

Additional customizations are described below:

### 4.7.1 Change Settings (Outlook)

You can choose **SpamSieve - Change Settings** from Outlook's **Scripts** menu to customize SpamSieve's behavior in Outlook.

The settings are:

- Should “Train as Spam” mark the messages as read?
- When you use “Train as Good” on a message in the spam folder, should the message be moved back to the inbox?
- When you use “Train as Good” on a message in the spam folder, should the message be marked as unread?
- Should incoming spam messages be marked with category “Uncertain Junk” rather than “Junk” if SpamSieve thinks they are not as spammy?

### 4.7.2 Duplicate Outlook Calendar Invitations

If you receive calendar invitations by e-mail and have Outlook set to automatically add them to your calendar, Outlook may see a good message that SpamSieve moves back from the **InboxSpamSieve** folder to **Inbox** as a new invitation. To prevent a duplicate calendar event from being created, you can set up your Outlook rules to not move the invitation e-mails to **InboxSpamSieve**. For example, you could add a rule above the SpamSieve rules that moves the invitation messages to another folder.

### 4.7.3 Outlook Keyboard Shortcuts

If you would like keyboard shortcuts for the training commands described in Step 7, you can set up the standard SpamSieve keyboard shortcuts as follows:

1. Download and install [FastScripts](#)<sup>47</sup>. (It is free for up to 10 keyboard shortcuts.)
2. Launch FastScripts.
3. From the FastScripts icon menu, go to the **FastScripts** submenu and choose **Preferences...**
4. Click on the **Script Shortcuts** tab.
5. In the **Microsoft Outlook** section, double-click on **(none)** in the **Shortcut** column next to **SpamSieve - Train as Good**. It will enter edit mode. Type Command-Control-G to set the shortcut.
6. In the **Microsoft Outlook** section, double-click on **(none)** in the **Shortcut** column next to **SpamSieve - Train as Spam**. It will enter edit mode. Type Command-Control-S to set the shortcut.

#### 4.7.4 Filtering Other Outlook Folders

You can use Outlook rules to automatically organize messages into folders. If you want SpamSieve to filter these additional folders (rather than just the inbox), create an additional SpamSieve inbox folder for each folder that you want to be filtered. For example, if you messages from **x@y.z** to end up in folder **XYZ**, create two folders: **XYZ** and **InboxSpamSieveXYZ**. Create an Outlook rule called **InboxSpamSieve (XYZ)** that moves the desired messages into folder **InboxSpamSieveXYZ**. When SpamSieve checks for new messages, it will move the good messages in **InboxSpamSieveXYZ** to **XYZ** and the spam messages to **Junk**.

#### 4.7.5 Spam Message Categories (Outlook)

SpamSieve colors spam messages in Outlook using one of two categories:

##### **Junk**

This is for messages that you mark as spam (using the **SpamSieve - Train as Spam** command) and for most incoming messages that SpamSieve thinks are spam.

##### **Uncertain Junk**

This is for incoming messages that SpamSieve thinks are spam, but whose scores are below the uncertainty threshold. For more information about scores and uncertainty, see the [A spam message is uncertain if](#) preference.

To change the colors associated with these categories, choose **Message** ▸ **Categorize** ▸ **Edit Categories...**

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

#### **Outlook 2011**

Normally, both **Junk** and **Uncertain Junk** messages are put into the same **Junk E-mail** folder. It is also possible to separate the messages by category. To do this:

<sup>47</sup><http://www.red-sweater.com/fastscripts/>

1. Create a new folder in Outlook called **Uncertain Junk**.
2. Create a third rule called **SpamSieve - Move Uncertain Messages**. It should say “If Category Is Uncertain Junk, Then Move message Uncertain Junk.”
3. Drag the new rule between the **SpamSieve - Set Category** and **SpamSieve - Move Messages** rules.

#### 4.7.6 Separate Spam Folders for Each Account (Outlook 2011)

Normally, SpamSieve puts the spam messages from all your Outlook 2011 accounts into a single folder called **Junk E-mail**.

If you want to have a separate spam folder for each account, first create the requisite empty folders.

Then, instead of the single **SpamSieve - Move Messages** rule described in the [Setting Up Outlook 2011](#) section, create *two* rules per account. For example:

1. SpamSieve - Move messages - *Account 1* - Junk

When a new message arrives: If all conditions are met:

- Category Is Junk
- Folder Is INBOX (*Account 1*)

Do the following:

- Move Message Junk E-mail (*Account 1*)

2. SpamSieve - Move messages - *Account 1* - Uncertain Junk

When a new message arrives: If all conditions are met:

- Category Is Uncertain Junk
- Folder Is INBOX (*Account 1*)

Do the following:

- Move Message Junk E-mail (*Account 1*)

And similarly create two rules for *Account 2*, etc.

## 4.8 Backing Up Messages

SpamSieve includes an experimental feature to save backup copies of the messages that it has processed. This includes new messages that were automatically filtered through it, as well as messages that you’ve manually trained. A backup can be useful because:

- A small percentage of users are running into [bugs in Apple Mail on macOS 10.15](#) that can cause messages to be deleted or turn blank when they’re moved. The bugs can manifest with or without SpamSieve installed. They can apply to messages that you drag and drop, as well as those that are moved by rules or by AppleScript.



- Even if your Mac and its mail program are functioning normally, another computer or device that accesses the same mail account could inappropriately move or delete some of the messages. These changes would then be synced back to your Mac.

To enable the backup:

- [Click here<sup>48</sup>](#) to enable automatic backups of good messages. [Click here<sup>49</sup>](#) to turn off the backup.
- [Click here<sup>50</sup>](#) to enable automatic backups of spam messages. [Click here<sup>51</sup>](#) to turn off the backup. You probably don't want to back up actual spam messages, but this could be useful if you are worried about SpamSieve incorrectly classifying a good message as spam and then something happening to the message before you can train it as good.

The backups are stored in the folders:

```
/Users/<username>/Library/Application Support/SpamSieve/Good Messages
/Users/<username>/Library/Application Support/SpamSieve/Spam Messages
```

There is one `.eml` file per message. The name of file is the message's identifier from [SpamSieve's log](#). You can find a particular message by viewing or searching SpamSieve's log to find the right identifier. Or you can sort the backup folder by date to easily view recent messages. This can also be useful if you want to delete older message backups that you no longer want to store.

Once you find a message's backup you can:

- View the message in the Finder using Quick Look.
- Double-click the file to open it in Apple Mail. You can use the **Message ▸ Copy Message** menu command to copy it into a mailbox in Mail's data store.
- Import the message into [EagleFiler](#), which can view and search `.eml` files as well as [merge them](#) into the standard mbox format.

## 5 Menus

### 5.1 The SpamSieve Menu

After clicking on SpamSieve's Dock icon, you will see the **SpamSieve** menu at the top-left of the screen, next to the Apple menu.

---

<sup>48</sup>`x-spamsieve://default?k=LogGood&v=YES`

<sup>49</sup>`x-spamsieve://default?k=LogGood&v=NO`

<sup>50</sup>`x-spamsieve://default?k=LogSpam&v=YES`

<sup>51</sup>`x-spamsieve://default?k=LogSpam&v=NO`

### 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](#).

Questions about SpamSieve may be sent to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>52</sup>. We're 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...](#) command.

### 5.1.2 Software Update...

#### Checking for Updates

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 **Check for updates automatically** checkbox.

#### Updating

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 downloads folder. Click **Download & Install** to have it download the `.dmg` and then update the installed SpamSieve application to the new version. For more information, please see [Updating From a Previous Version](#).

#### Installing a Fresh Copy

You can hold down the Option key when you click **Check Now** to make SpamSieve always download the latest version, even if your version is already up-to-date. This is an easy way to download and re-install a fresh copy of SpamSieve if your copy is damaged.

#### Privacy

To check for a new version, SpamSieve contacts a Web server at `c-command.com` over a secure connection. SpamSieve transmits the following information to the server: the name of the product (SpamSieve) and its version, the version of macOS, the kind of Mac and processor, whether SpamSieve has been purchased, whether it is running in dark mode, the name and version 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.

#### Mac App Store

If you purchased DropDMG or EagleFiler via the Mac App Store, the **Software Update...** menu command is not present, and updates are available via the **App Store** application.

---

<sup>52</sup><mailto:spamsieve@c-command.com>

### 5.1.3 Purchase...

When you launch SpamSieve for the first time, the **Purchase** window will automatically open. You can also open it by choosing **Purchase...** from the **SpamSieve** menu.

#### Trial/Demo Period

SpamSieve has a free trial. During the trial period, SpamSieve is fully functional; the only difference in behavior is that it will periodically remind you that you are using the trial. To use SpamSieve in trial mode, you can simply close the **Purchase** window.

The trial period lasts for 30 days. (After the 30 days, if you haven't had a chance to use SpamSieve very much, you can continue using it for up to a total of 7 launches.) To use SpamSieve beyond the trial period, you must purchase it. This entitles you to free updates and support.

#### Purchasing

Click the **Purchase Online** button to enter the [online store](#).

#### After Purchasing

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**. You do not have to "install the purchased version"; rather, SpamSieve will then know that you have purchased and you can keep using it as before—with all the preferences that you had set and data that you had entered.

#### Reinstalling a Previous Purchase

If you need to re-install SpamSieve, you can simply re-enter your **Serial Name** and **Serial Number** and click **Personalize**; there's no need to purchase again.

If you cannot find your serial number, click the **Look Up My Serial Number** button. This will open a form where you can enter your e-mail address and look up your order information.

#### License Information

A license for SpamSieve is good for one person *or* one computer. This means that you can use it on your desktop Mac and your laptop, or you and your family can use it (in separate user accounts) on a shared Mac. If there are multiple users on multiple Macs, you should purchase multiple licenses. Discounts for packs of 2, 10, and 50 licenses are available above. A family (all living in the same household) can share a 2-user license. If you already have a single license, you can upgrade to a family license. To do this, e-mail your old order number to [sales@c-command.com](mailto:sales@c-command.com)<sup>53</sup>, and we'll send you a coupon code.

#### Upgrade Policy

All maintenance releases (1.0.1, 1.0.2, 1.6.1, etc.) and minor feature updates (1.1, 1.2, 1.5, etc.) are free. We have a track record of many such updates, and they have included significant new features. Major upgrades (2.0, 3.0) are free if you purchased the previous version within the last six months. If you purchased longer ago than that, you get a discount. (Note: The upgrade discounts are only available if you originally purchased direct from C-Command, since the Mac App Store does not support upgrades.)

---

<sup>53</sup><mailto:sales@c-command.com>

## Mac App Store

The **Purchase...** menu command is not present if you purchased via the [Mac App Store](#). In that case, there is no trial period, and licensing is based on your iTunes account rather than the number of people or computers.

### 5.1.4 Mac App Store

Due to Apple's store guidelines, SpamSieve is currently not available from the [Mac App Store](#)<sup>54</sup>. It can be purchased [direct from C-Command](#).

### 5.1.5 Install Apple Mail Plug-In

*Note:* You may need to [show SpamSieve's Dock icon](#) in order to access [the SpamSieve menu](#) and this command.

The **Install Apple Mail Plug-In** command installs (or updates) the plug-in that SpamSieve uses to integrate with Apple Mail. If the plug-in is successfully installed, you will see the SpamSieve commands in Mail's **Message** menu. For more information, see the [Setting Up Apple Mail](#) and [Why don't I see the SpamSieve commands in Apple Mail's Message menu?](#) sections of the manual.

### 5.1.6 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 should fix that problem.

This command also makes sure that you have an Entourage category called **Uncertain Junk**.

For more information, see the [Setting Up Entourage](#) section of the manual.

### 5.1.7 Install Outlook Scripts

This command installs (or updates) the AppleScript files that SpamSieve uses to integrate with Outlook.

This command also makes sure that you have an Outlook category called **Uncertain Junk**.

For more information, see the [Setting Up Outlook](#) section of the manual.

---

<sup>54</sup><http://www.apple.com/osx/apps/app-store.html>

### 5.1.8 Show Other Scripts

This opens a folder containing AppleScript files for integrating SpamSieve with DragThing, 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 and Outlook, as well as SpamSieve’s plug-in for Apple Mail. 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.

### 5.1.9 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 Contacts (previously Address Book). The “Me” card has “me” written on top of the picture; to find it, choose **Go to My Card** from the **Card** menu. 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.

### 5.1.10 Uninstall Apple Mail Plug-In...

This command will prompt you to remove any SpamSieve Mail rules, then uninstall the SpamSieve plug-in and launch agent. The SpamSieve application and training data files will remain. SpamSieve will then quit Mail itself so that the plug-in code is unloaded.

For more information, see the [Uninstalling SpamSieve](#) section.

If you no longer want to use SpamSieve with Mail (e.g. because you are now using a different mail client), you can choose **Uninstall Apple Mail Plug-In...** from the **SpamSieve** menu. This will prevent SpamSieve from reminding you to enable the Mail plug-in.

## 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.

This feature is usually not needed, as SpamSieve will automatically create whitelist and blocklist rules based on the messages that you receive.

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 Outlook, choose **Export...** from the **File** menu and select the option for **Contacts to a list (tab-delimited text)**.
- To import addresses from the macOS address book, open the **Contacts** (previously **Address Book**) program. Select all the names in the middle column 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 macOS address book instead of using the [Use macOS Contacts](#) preference, or why you would import addresses from Entourage or Outlook instead of using the [Use Entourage/Outlook 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](#) to convert the rules into address book cards.

## 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...

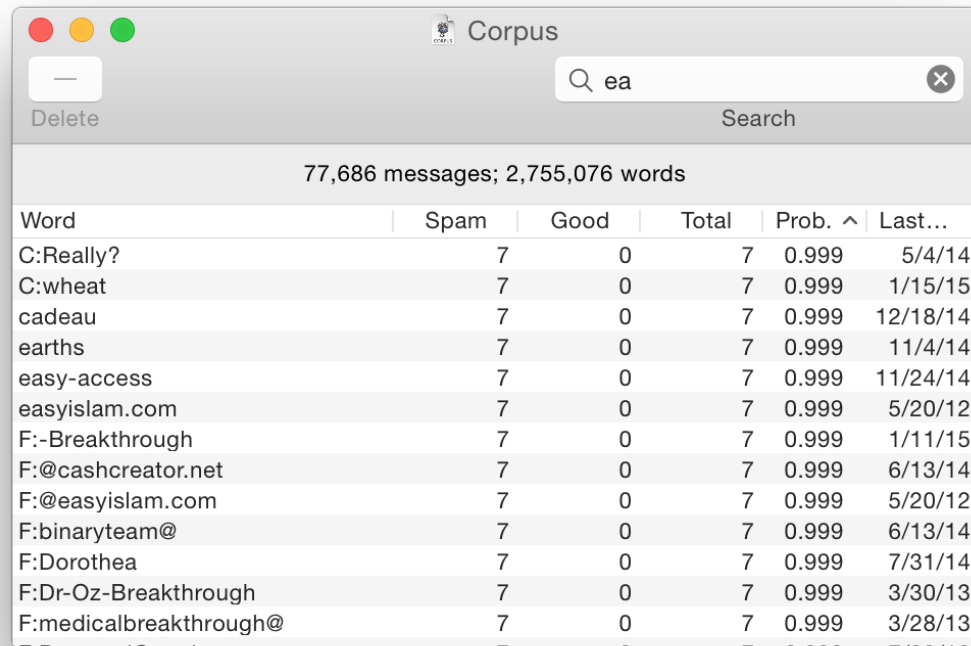
This exports the active [corpus](#) to XML format. You might do this in order to [import](#) the corpus on another machine.

# 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.



| Word                   | Spam | Good | Total | Prob. ^ | Last...  |
|------------------------|------|------|-------|---------|----------|
| C:Really?              | 7    | 0    | 7     | 0.999   | 5/4/14   |
| C:wheat                | 7    | 0    | 7     | 0.999   | 1/15/15  |
| cadeau                 | 7    | 0    | 7     | 0.999   | 12/18/14 |
| earths                 | 7    | 0    | 7     | 0.999   | 11/4/14  |
| easy-access            | 7    | 0    | 7     | 0.999   | 11/24/14 |
| easyislam.com          | 7    | 0    | 7     | 0.999   | 5/20/12  |
| F:-Breakthrough        | 7    | 0    | 7     | 0.999   | 1/11/15  |
| F:@cashcreator.net     | 7    | 0    | 7     | 0.999   | 6/13/14  |
| F:@easyislam.com       | 7    | 0    | 7     | 0.999   | 5/20/12  |
| F:binaryteam@          | 7    | 0    | 7     | 0.999   | 6/13/14  |
| F:Dorothea             | 7    | 0    | 7     | 0.999   | 7/31/14  |
| F:Dr-Oz-Breakthrough   | 7    | 0    | 7     | 0.999   | 3/30/13  |
| F:medicalbreakthrough@ | 7    | 0    | 7     | 0.999   | 3/28/13  |

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/
```

(See the [How can I open the Library folder?](#) section.) 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:

#### **Filtered Mail**

##### **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.



## **SpamSieve Accuracy**

### **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.

## **Corpus**

### **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](#).

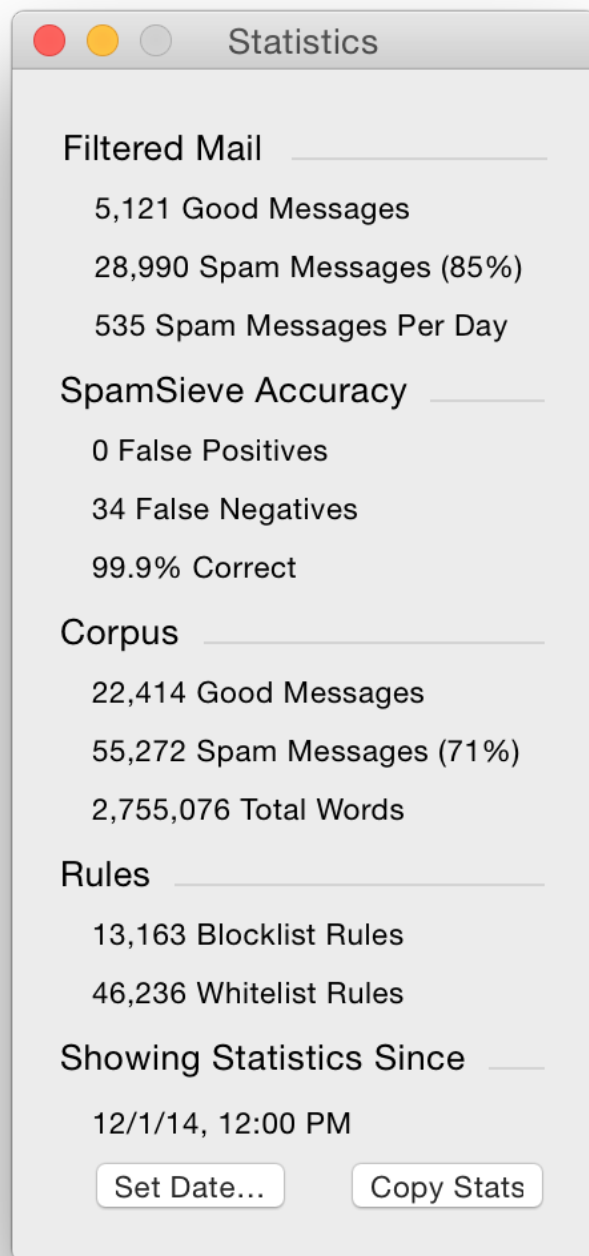
## **Rules**

### **Blocklist Rules**

The number of rules on SpamSieve's [blocklist](#).

### **Whitelist Rules**

The number of rules on SpamSieve's [whitelist](#).



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 also accept dates specified in natural language, such as “last Sunday at dinner” or “today.” The **Now** button enters the current date and time.

If you’ve chosen a suitable date and the “Filtered Messages” section shows zero filtered messages, that means that your mail program did not ask SpamSieve to filter any incoming messages. You should check to make sure that the mail program [setup](#) is correct.

### 5.3.4 Open Log

SpamSieve keeps a log of which messages it has filtered, which messages you’ve trained it with, and any errors that have occurred. The **Open Log** command in the **Filter** menu 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.

#### “Predicted: Good/Spam” Log Entries

For each incoming message, there should be a log entry that says **Predicted: Good** or **Predicted: Spam**. Here are some questions that these entries can help you answer:

1. Why did a particular spam message make it to my inbox?
  - a) If there is no **Predicted: Good** log entry for the message, SpamSieve was never given a chance to analyze it.
    - Check the setup of your mail program, as described in the [Why is SpamSieve not catching my spam?](#) section.
  - b) If there is a **Predicted: Good** log entry for the message, the **Reason** will say why SpamSieve thought the message was good. For example:
    - 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 macOS Contacts](#). See also the [How do I make SpamSieve catch spams sent from my own address?](#) section.
    - If it says **sender <address> in Entourage/Outlook 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/Outlook address book](#).
    - If it says **<From (address) Is Equal to "[...]"> in SpamSieve whitelist**, SpamSieve thought the message was good because (a) you had trained a previous message from that sender as good, or (b) you had received a previous message from that sender, SpamSieve thought it was good for other reasons, and you had not trained the message as spam (see the [Correct All Mistakes](#) section).
    - If spam messages are being predicted as good and you don’t understand why, please [send in a report](#).

## 2. Why is a particular good message in my spam mailbox?

- a) If there is no **Predicted: Spam** log entry for the message, SpamSieve did not move the message out of the inbox. In fact, SpamSieve was never even given a chance to analyze the message.
  - [Check the setup](#) in your mail program to make sure that the built-in junk mail filter is disabled and that SpamSieve is the only rule that moves messages to the spam mailbox.
  - Check the [Why is every message going to the Spam mailbox?](#) section to see if any of those items apply to you.
  - Check the [How should I configure the junk filter on my mail server?](#) section in case the message is being classified as spam before it even gets to your Mac.
- b) If there is a **Predicted: Spam** log entry for the message, the **Reason** will say why SpamSieve thought the message was spam.
  - If good messages are being predicted as spam and you don't understand why, please [send in a report](#).

### “Trained: Good/Spam (Manual)” Log Entries

These log entries represent messages that you had trained as good or spam using the menu commands in your mail program.

### “Trained: Good/Spam (Auto)” Log Entries

These log entries represent messages that SpamSieve auto-trained. It's normal for SpamSieve to auto-train a message as good if it thinks that the message isn't spam. This will add the sender to the whitelist to ensure that future messages from that sender get through to your inbox. If you later train the message as spam, SpamSieve will disable (uncheck) the whitelist rule. Thus, auto-training should not ordinarily cause problems unless you receive a large flurry of messages from the same sender address, or if you forget to train the message as spam and then the address remains enabled on the whitelist. For more information, see the [Auto-train with incoming mail](#) section.

### Searching the Log

If you have a question about a particular message, you can search the log to see whether there's a **Predicted** entry for it. It's best to search the log using Console's **Edit ▸ Find ▸ Find...** command, rather than the **Filter** search field in the toolbar.

You may also find it easier to search by using the [Edit Log](#) command.

### Accessing the Log Files

SpamSieve stores its log in the folder:

```
/Users/<username>/Library/Logs/SpamSieve/
```

(See the [How can I open the Library folder?](#) section.) If you find that the logs are taking up too much disk space, you can delete the .bz2 files at any time.

### Help With the Log

The [Sending in the SpamSieve Log File](#) section describes how you can e-mail your log file to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>55</sup> if you need help interpreting it.

### 5.3.5 Edit Log

This command opens the [log file](#) in a text editor such as TextEdit or [TextWrangler](#)<sup>56</sup> instead of Console. This makes it easier to read and search large log files. You can control which editor SpamSieve uses by choosing **Get Info** in the Finder on a `.txt` file, changing the application in the **Open with** pane, and pressing **Change All**.

### 5.3.6 Show Blocklist

The **Show Blocklist** command in the **Filter** menu opens the **Blocklist** window. The blocklist consists of a list of *rules*. If a message *matches* one or more enabled rules on the blocklist (and [Use SpamSieve blocklist](#) is checked), SpamSieve will predict that it is spam. As always, SpamSieve does not prevent you from *receiving* the spam messages; rather, the blocklist ensures that they will go to the spam mailbox rather than the inbox. You can also configure Apple Mail so that the blocklisted messages [go directly to the trash](#).



| Date     | Header               | Match Style   | Text to Match                         | ✓ | Hits  |
|----------|----------------------|---------------|---------------------------------------|---|-------|
| 9/17/08  | From (address)       | Is Equal to   | retsnewe@tacotex.be                   | ✓ | 0     |
| 2/11/08  | From (address)       | Is Equal to   | postmaster@mmsreply.t-mobile.co.uk    | ✓ | 0     |
| 4/18/11  | From (address)       | Is Equal to   | oftayphgtf@agentk-12.org              | ✓ | 0     |
| 2/13/08  | From (name)          | Is Equal to   | Robin Morrow                          | ✓ | 0     |
| 6/9/14   | From (name)          | Is Equal to   | Gift Cards                            | ✓ | 10    |
| 6/13/08  | From (name)          | Is Equal to   | consalve joaquim                      | ✓ | 0     |
| 12/6/10  | From (address)       | Is Equal to   | fbmessage+pp-...acebookmail.com       | ✓ | 2     |
| 1/8/07   | From (address)       | Is Equal to   | Mailer-Daemon@...xcore20.plus.net     | ✓ | 3     |
| 10/17/07 | From (address)       | Is Equal to   | DoNotReply@harmonsgrocery.com         | ✓ | 1     |
| 3/11/13  | From (name)          | Is Equal to   | ¼ö ää»                                | ✓ | 0     |
| 11/16/06 | Body (any text part) | Matches Regex | <BODY[^>]*>\s*<IMG[^>]*"cid:[^>]*>    | ✓ | 7,601 |
| 10/26/06 | Body (any text part) | Matches Regex | (?s)<DIV[^>]*>.*?...IV[^>]*>.*?</DIV> | ✓ | 1,124 |
| 10/18/06 | Body (any text part) | Matches Regex | <body bgcolor="...g alt=" src="cid:   | ✓ | 1,742 |

The counterpart to the blocklist is the [whitelist](#).

### Creating Rules

<sup>55</sup><mailto:spamsieve@c-command.com>

<sup>56</sup><http://www.barebones.com/products/textwrangler/>

There is normally no need for you to manually create or delete blocklist rules because SpamSieve [learns](#) to recognize your spam automatically. Thus, it's OK if you receive spam from constantly changing addresses; you don't have to worry about creating blocklist rules to match all of them. If a lot of spam is in your inbox, your first step should be to follow the instructions in [Why is SpamSieve not catching my spam?](#) rather than to create blocklist rules that may not be needed or even used (e.g. if the real problem is that your mail program isn't set up properly).

## Rules and Training

By default, the [Train SpamSieve blocklist](#) preference is enabled. This means that SpamSieve will automatically create blocklist rules when you train a message as spam. You won't get spam from the same address or sender name twice.

SpamSieve will also disable (uncheck) matching blocklist rules when you train a message as good. This prevents a bad blocklist rule from blocking similar good messages.

## Editing Rules

You can edit a rule's **Header** or **Match Style** by clicking in the corresponding column and choosing from the pop-up menu. To edit a rule's **Text to Match**, double-click the text. For more information about the available options see the [Rule Columns, Headers, and Match Styles](#) section.

## Deleting and Disabling Rules

You can delete a rule from the blocklist by selecting it and pressing Delete. Generally, there is little reason to delete rules. SpamSieve is optimized such that having lots of rules does not reduce performance.

If you don't like what a rule is doing, you should uncheck the rule rather than deleting it. This will prevent SpamSieve from re-learning the rule automatically (see "Rules and Training" above). 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 spam 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, so SpamSieve will still be able to catch that spam. 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 would prevent those spam messages from being caught.

## Blocklisting Domains and Countries

You can tell SpamSieve to classify every message from a particular domain as spam. For example, to block every message from Spammy Company, open the **Blocklist** window, click the + button, and create a rule that says **From (address) Ends With @spammycompany.com**. You can also create rules for particular countries. For example, to block every message from an e-mail address in Nigeria, create a rule that says **From (address) Ends With .ng**

## Blocking Messages to Invalid Addresses

If you have your own domain name, it's best to configure the server not to have a [catch-all address](#)<sup>57</sup> because that would lead to your receiving spam messages sent to addresses that are not even valid. SpamSieve could filter out those spams, but it's better if you can avoid downloading them and cluttering your spam mailbox in the first place.

---

<sup>57</sup><http://en.wikipedia.org/wiki/Catch-all>

If you cannot configure your server in that way, [you can](#) use the **Matches Regex** match style to create a blocklist rule that matches messages sent to invalid addresses at your domain. For example, this regex:

```
^.*(?
```

would match all messages where the match field ends with @domain.com but is not sales@domain.com or support@domain.com.

## Finding Rules

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.

## Exporting Addresses

You can use the [Copy Whitelist/Blocklist Addresses script](#) to get a list of addresses, e.g. to add to the configuration of a server-side spam filter.

## Troubleshooting Rules

Blocklist rules will not match a message if:

- One of the [Filters](#) above the blocklist classified the message as good.
- The blocklist rule is disabled.
- The mail program did not send the message to SpamSieve for analysis. See the [Why is SpamSieve not catching my spam?](#) section.

### 5.3.7 Rule Columns, Headers, and Match Styles

This section explains the options available for each rule in SpamSieve's [blocklist](#) and [whitelist](#) windows.

#### Rule Columns

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.

##### **✓ (Enabled)**

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. (See [Rules and Training](#).)

**Hits**

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

**Rule Headers**

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](http://www.iana.org/assignments/character-sets)<sup>58</sup>.

## 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.

## Rule Match Styles

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.

### 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](http://en.wikipedia.org/wiki/Regular_expressions)<sup>59</sup> [regular expression](http://pcre.org/pcre.txt)<sup>60</sup>. 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.

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.

---

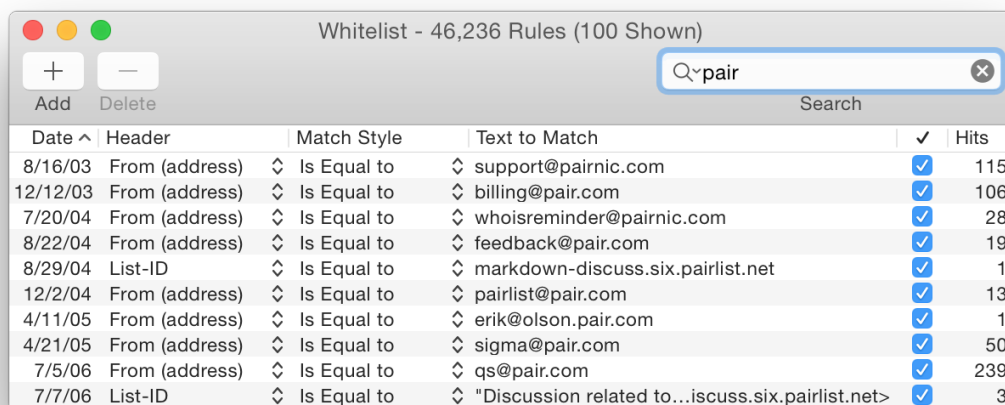
<sup>58</sup><http://www.iana.org/assignments/character-sets>

<sup>59</sup><http://pcre.org/pcre.txt>

<sup>60</sup>[http://en.wikipedia.org/wiki/Regular\\_expressions](http://en.wikipedia.org/wiki/Regular_expressions)

### 5.3.8 Show Whitelist

The **Show Whitelist** command in the **Filter** menu opens the **Whitelist** window. The whitelist consists of a list of *rules*. If a message *matches* one or more enabled rules on the whitelist (and [Use SpamSieve whitelist](#) is checked), SpamSieve will predict that it is good. The whitelist is most commonly used for matching messages sent from particular addresses, domains, or mailing lists.



| Date ^   | Header         | Match Style   | Text to Match                                       | ✓ | Hits |
|----------|----------------|---------------|---|---|------|
| 8/16/03  | From (address) | ↕ Is Equal to | ↕ support@pairnic.com                               | ✓ | 115  |
| 12/12/03 | From (address) | ↕ Is Equal to | ↕ billing@pair.com                                  | ✓ | 106  |
| 7/20/04  | From (address) | ↕ Is Equal to | ↕ whoisreminder@pairnic.com                         | ✓ | 28   |
| 8/22/04  | From (address) | ↕ Is Equal to | ↕ feedback@pair.com                                 | ✓ | 19   |
| 8/29/04  | List-ID        | ↕ Is Equal to | ↕ markdown-discuss.six.pairlist.net                 | ✓ | 1    |
| 12/2/04  | From (address) | ↕ Is Equal to | ↕ pairlist@pair.com                                 | ✓ | 13   |
| 4/11/05  | From (address) | ↕ Is Equal to | ↕ erik@olson.pair.com                               | ✓ | 1    |
| 4/21/05  | From (address) | ↕ Is Equal to | ↕ sigma@pair.com                                    | ✓ | 50   |
| 7/5/06   | From (address) | ↕ Is Equal to | ↕ qs@pair.com                                       | ✓ | 239  |
| 7/7/06   | List-ID        | ↕ Is Equal to | ↕ "Discussion related to...iscuss.six.pairlist.net> | ✓ | 3    |

The counterpart to the whitelist is the [blocklist](#).

### Creating Rules

There is normally no need for you to manually create or delete whitelist rules because SpamSieve learns to recognize your good automatically. If a lot of good messages are in your **Spam** mailbox, your first steps should be to [check the setup in your mail program](#) and to [check the log](#) rather than to create whitelist rules.

### Rules and Training

By default, the [Train SpamSieve whitelist](#) preference is enabled. This means that SpamSieve will automatically create whitelist rules when you train a message as good. Once you receive one good message from a person, all future messages will get through to your inbox.

SpamSieve will also disable matching whitelist rules when you train a message as spam. This prevents a bad whitelist rule from letting through similar spam messages.

By default, the [Auto-train with incoming mail](#) preference is enabled. This means that if you receive a message that SpamSieve thinks is good, SpamSieve will automatically add whitelist rules so that future messages from that same sender are also classified as good. Thus, it is important to [correct all the mistakes](#) to avoid having incorrect whitelist rules.

### Editing Rules

You can edit a rule's **Header** or **Match Style** by clicking in the corresponding column and choosing from the pop-up menu. To edit a rule's **Text to Match**, double-click the text. For more information about the available options see the [Rule Columns, Headers, and Match Styles](#) section.

## Deleting and Disabling Rules

You can delete a rule from the whitelist by selecting it and pressing Delete. Generally, there is little reason to delete rules. SpamSieve is optimized such that having lots of rules does not reduce performance.

## Spammy Whitelist Rules

It is normal to see spammy rules on the whitelist that are unchecked. This is because of [auto-training](#). When SpamSieve thinks an incoming message is good, SpamSieve also adds a rule to the whitelist. SpamSieve may be wrong about that message, and that's OK. If SpamSieve makes a mistake and lets a spam message through, when you train the message as spam it will disable the corresponding whitelist rules. The rules will then be shown as unchecked. A disabled rule won't match any messages, so it won't cause any spam to get through.

If you see spammy rules that are checked, this is not normal. It means that you have not been [correcting all the mistakes](#).

Do not delete spammy whitelist rules. This is almost never a good idea:

- If the rules are disabled, you should leave them in place to prevent SpamSieve from creating those incorrect rules again in the future.
- If the rules are enabled, you should find the spam messages from those addresses and train them as spam. Not only will this disable the rules, but it will also update SpamSieve's corpus and statistics.

## Whitelisting Domains

You can tell SpamSieve to classify every message from a particular domain as good. For example, to whitelist every message from Apple, open the **Whitelist** window, click the + button, and create a rule that says **From (address) Ends With @apple.com**.

## Mailing List Messages

The whitelist 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.

## Codewords

You can 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*.

## Finding Rules

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.

## Exporting Addresses

You can use the [Copy Whitelist/Blocklist Addresses script](#) to get a list of addresses, e.g. to add to the configuration of a server-side spam filter.

## Troubleshooting Rules

Whitelist rules will not match a message if:

- One of the [Filters](#) above the whitelist classified the message as spam.
- The whitelist rule is disabled.
- The mail program did not send the message to SpamSieve for analysis. See the [Open Log](#) section.

### 5.3.9 Add Rule

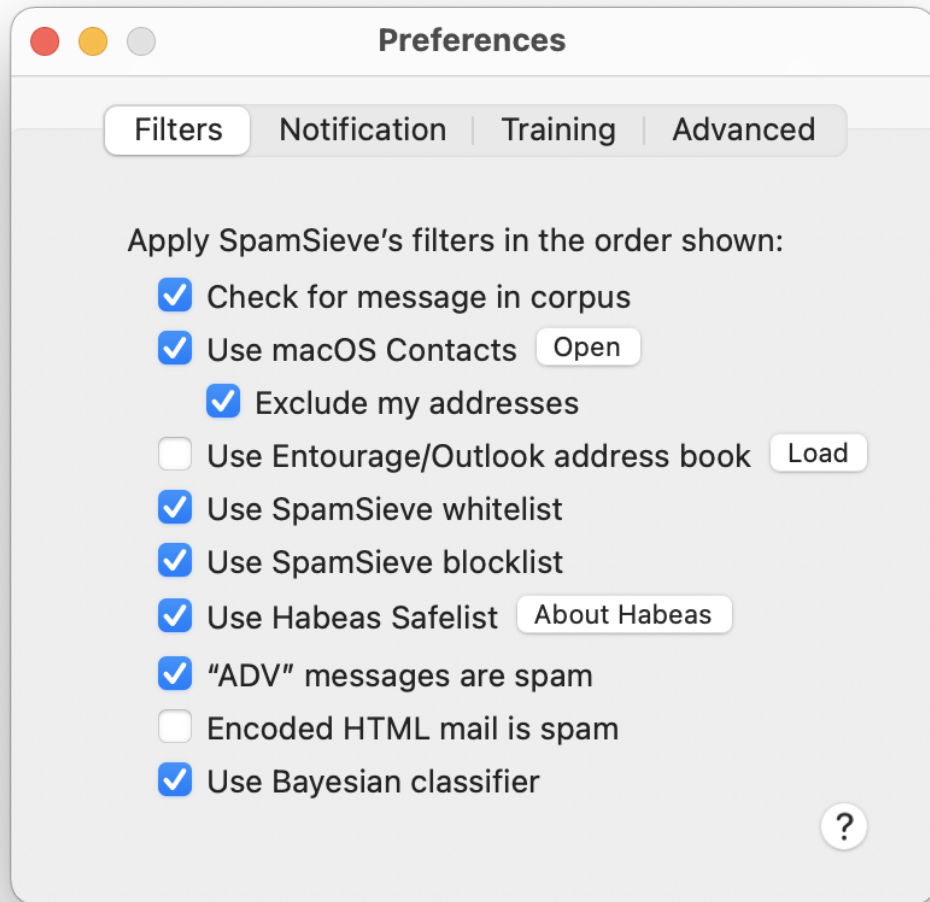
This command creates a new rule in either the [whitelist](#) or [blocklist](#). This is useful if you want to add your own rules to the whitelist or blocklist, rather than having SpamSieve learn the rules when you train it with messages. For example, you could create a blocklist rule to catch spam messages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

## 6 Preferences

To access the preferences, click on the SpamSieve icon in the Dock. Then choose **Preferences...** from the **SpamSieve** menu at the top of the screen (next to the Apple menu).

### 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. This is especially useful when testing the setup in your mail program. 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 macOS Contacts

With this option enabled, SpamSieve will never predict a message to be spam if its sender's e-mail address is in the Contacts (previously Address Book) application.

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

If spam messages get through to your inbox because they are sent from addresses in your address book, you can either uncheck **Use macOS Contacts** or see the [Exclude my addresses](#) section. For more information, please see the [How do I make SpamSieve catch spams sent from my own address?](#) section.

#### Access to Your Contacts

The first time you use SpamSieve to filter messages, it will ask for permission to access your contacts. You can change the access setting by opening System Preferences, going to the **Security & Privacy** pane, clicking on the **Privacy** tab, clicking on **Contacts** in the list, and checking or unchecking **SpamSieve.app**. (Please note that the applications in the list are *not* sorted alphabetically.)

#### Repeated Access Prompts

If the system keeps asking you for permission to access your contacts and does not remember this between launches:

- You may need to reset the privacy database by entering this command in Terminal:

```
tccutil reset AddressBook
```

- Your copy of SpamSieve may be damaged. Please see the [Reinstalling a Fresh Copy](#) section.

#### Mail Client Address Books

Entourage users may prefer to use Entourage's address book as a whitelist instead of Apple's. This is described in the [Setting Up Entourage](#) section.

PowerMail users should be sure to enable the option to use Apple's address book.

### 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 Contacts (previously Address Book) application 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 macOS Contacts](#) 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 Contacts, 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.

For more information, please see the [How do I make SpamSieve catch spams sent from my own address?](#) section.

### Excluding Extra Addresses

You can use Terminal to add additional addresses that you want to exclude but that are not listed on the “Me” card. Enter a command such as:

```
defaults write com.c-command.SpamSieve ExtraAddressesToExclude -array a@b.com d@e.com
```

To remove the list of addresses to exclude, enter this command:

```
defaults delete com.c-command.SpamSieve ExtraAddressesToExclude
```

Changes take effect the next time you launch SpamSieve. You can see which extra addresses are excluded by entering this command:

```
defaults read com.c-command.SpamSieve ExtraAddressesToExclude
```

#### 6.1.4 Use Entourage/Outlook 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 contacts list for Entourage or Outlook. When you install SpamSieve, you should click the **Load** button to make SpamSieve read in the addresses in the Entourage or Outlook address book. 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.

### Re-loading Addresses

Whenever you *add* addresses to the Entourage or Outlook address book, you should go back to SpamSieve’s preferences and click **Load** so that SpamSieve learns about the new addresses. (This is not necessary for addresses that have already sent you e-mails, as SpamSieve will automatically see those messages and add the addresses to its whitelist.)

If you *remove* addresses from the Entourage or Outlook 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 or Outlook is downloading and filtering mail, as this may cause it to freeze.

### Your Own Addresses

If you have [Exclude my addresses](#) checked, addresses on the macOS Contacts app’s “Me” card will not be checked against Entourage or Outlook’s address book. This helps prevent forged spams from getting through. For more information, please see the [How do I make SpamSieve catch spams sent from my own address?](#) section.

## Multiple Identities

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

## Sync Services

Prior to macOS 10.8, Entourage and Outlook could automatically synchronize their address books with the system address book using a technology called Sync Services. SpamSieve could access the system address book directly, so there was no need for SpamSieve to load the addresses from Entourage or Outlook. As of macOS 10.8, Apple has deprecated Sync Services, and customers report that it no longer works reliably. Thus, it is recommended that you use the **Use Entourage/Outlook address book** option instead.

### 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](#) 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
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<sup>61</sup> or unencoded HTML messages.

### 6.1.10 Use Bayesian classifier

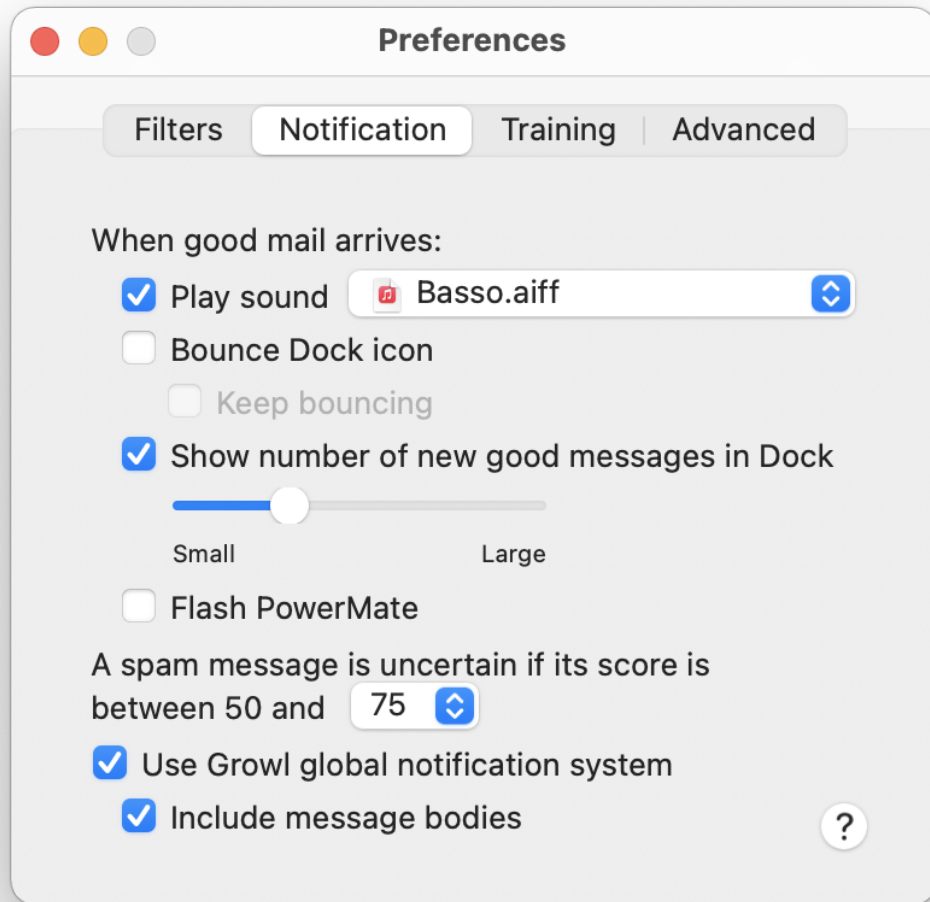
This enables SpamSieve’s main spam detector, which uses the [corpus](#) and [word probabilities](#) to identify spam messages. If you uncheck **Use Bayesian classifier**, SpamSieve will stop examining the full contents of the incoming messages, so this should only be done for testing purposes.

## 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.

---

<sup>61</sup><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 (as described in the [Notification](#) section). To add a sound to the menu, copy the sound file to the **Sounds** folder in your **Library** folder. (See the [How can I open the Library folder?](#) section.) SpamSieve will also look for sounds that are built into your installed e-mail programs.

You can adjust the **Alert volume** in the **Sound Effects** tab of the **Sound** pane in System Preferences. If the volume is set to zero, the Mac flashes the screen instead of playing the sound.

If you are not hearing the sounds, make sure that you have selected an appropriate speaker in the **Play sound effects through** pop-up menu.

### 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. “New” means “since the last time the number was reset”; it’s not related to the number of messages that are unread. “Good messages” means “messages for which there is a **Predicted: Good** entry in [SpamSieve’s log](#).”

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](#)<sup>62</sup> 5.3 or later, SpamSieve can show the message count in its tile in DragThing’s process dock.

### 6.2.5 Flash PowerMate

If you have a Griffin [PowerMate](#)<sup>63</sup>, this option will make it flash when new good messages arrive. The flashing will stop when you activate SpamSieve or your mail program.

This feature is compatible with version 3.0 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. The farther the score is away from the middle (50), the more confident SpamSieve is about whether the message is spam. Put another way, if you are trying to double-check SpamSieve’s work, you should focus your attention on the messages with scores closer to 50. If SpamSieve has made any mistakes, it is more likely to be with messages scored at 70 or 30 than with those scored at 95 or 5.

Spam messages that SpamSieve thought were good (false negatives) are generally easy for humans to spot. They tend to stick out amongst lots of good messages in the inbox.

---

<sup>62</sup><http://www.dragthing.com>

<sup>63</sup><http://store.griffintechology.com/powermate>

Good messages that SpamSieve thought were spam (false positives) are harder to spot. They can be buried amongst piles of messages in the spam folder. To help you find these messages, SpamSieve can notify you about *uncertain* spam messages, i.e. the messages in the spam folder that you should focus your attention on.

The pop-up menu lets you control the range of scores that SpamSieve considers to be uncertain. For example, if you set it to 75 (the default), messages that SpamSieve thought were spam but which have scores below 75 will be considered uncertain.

- Growl will show a notification bubble for each uncertain message. For more information, see the [Use Growl global notification system](#) section.
- In Outlook, the uncertain messages will be categorized as **Uncertain Junk** instead of **Junk** and will appear in a different color. For more information, see the [Spam Message Categories \(Outlook\)](#) section.

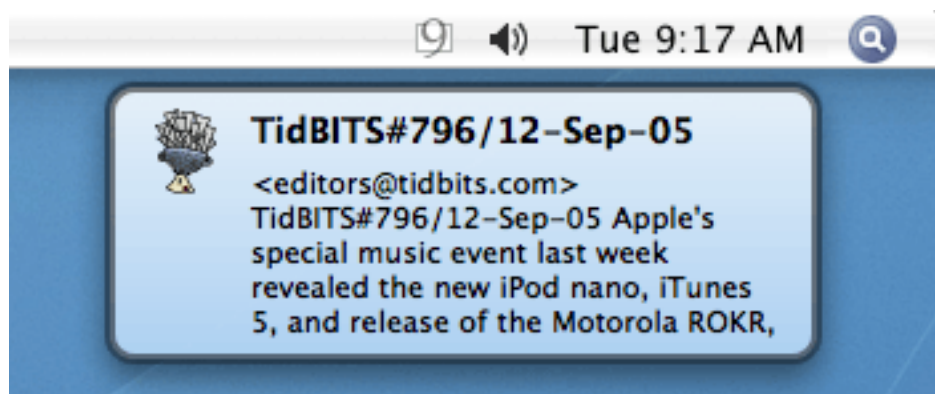
By making it easier to spot uncertain messages, these mechanisms help you to efficiently verify whether SpamSieve has filtered your mail correctly.

Uncertain messages are considered to be spam, unless you tell SpamSieve otherwise, so you should not train SpamSieve that they are spam.

### 6.2.7 Use Growl global notification system

[Growl](#)<sup>64</sup> is a third-party application 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. If you are not using Growl, turn off this option in order to improve performance.

Growl is not available on Apple Silicon Macs, unless SpamSieve is running in Rosetta (which is not recommended due to a macOS bug).



The following notifications are available:

#### Good Message Count

---

<sup>64</sup><http://www.growl.info>

This notification mimics the red number in SpamSieve's Dock icon (see [Show number of new good messages in Dock](#)). 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.

#### 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. For more information, see the [A spam message is uncertain if](#) preference. 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. Clicking to close the notification does not change whether SpamSieve thinks the message is spam. For messages that are actually spam, you don't need to do anything. For messages that are not spam, you should find the message in your mail program's spam mailbox and train it as good.

You can customize the notification style and enable/disable notifications:

#### Growl 2.x

Open the Growl application and choose **Preferences...** from the **Growl** menu. Click on the **Applications** tab and select **SpamSieve** at the left of the window.

#### Growl 1.3.x

Choose **Open Growl Preferences...** from the Growl menu.

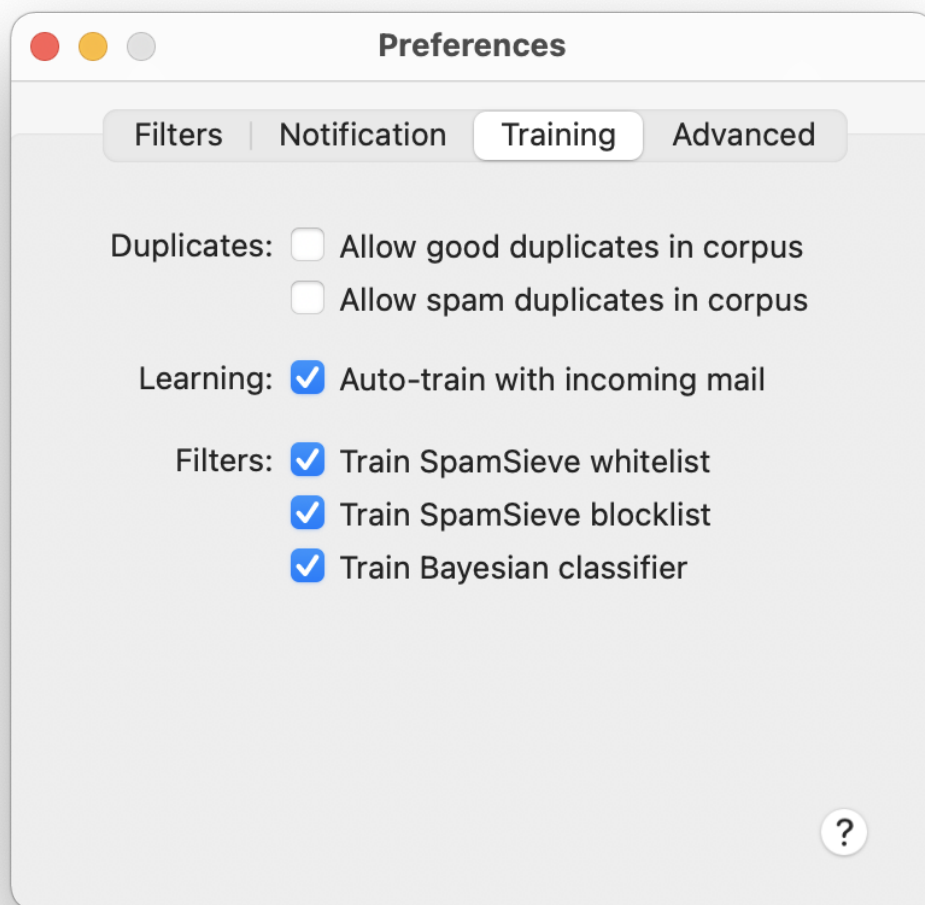
#### Growl 1.2

Open the Growl pane in System Preferences.

### 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. The whitelist will stay up-to-date so that messages from previous correspondents are never marked as spam. Also, 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.

#### Unable to Correct Mistakes

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.

#### Multiple Copies of SpamSieve

If you are using multiple copies of SpamSieve (on different Macs) to filter the same IMAP account, it's hard to know which one(s) to correct when a mistake is made. With auto-training off, you don't have to worry about that.

#### 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.

#### Delayed Corrections

If it will be a long time between when SpamSieve filters some messages and when you can correct any mistakes, the situation is similar to Bulk Processing, so you may want to turn off auto-training. If you'll be away from your SpamSieve Mac but have other mail access, you can eliminate the delay by using *remote training*. See the [Setting Up a Spam Filtering Drone](#) section.

### 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](#). This will make SpamSieve classify all future messages from that sender as good. Training SpamSieve with a spam message will disable the name and address if they appear in the whitelist (unless you've changed `DisableWhitelistRules` in the [esoteric preferences](#)).

#### 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**

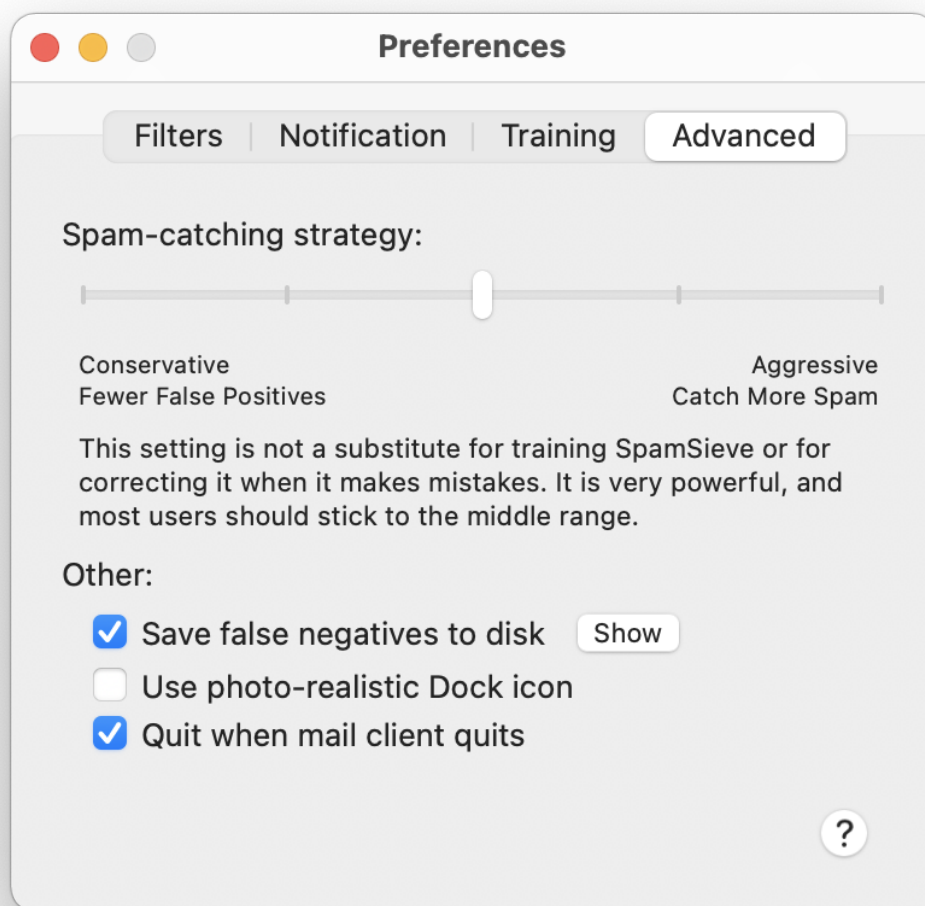
With this option enabled, training SpamSieve with a spam message will add the message sender's name and address to SpamSieve's [blocklist](#). This will make SpamSieve classify all future messages from that sender as spam. Training SpamSieve with a good message will disable the sender's name and address 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.



## 6.4 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 in the [Advanced](#) preferences opens the folder containing the saved messages. You can e-mail this folder, along with SpamSieve's [log file](#), to [spamsieve-fn@c-command.com](mailto:spamsieve-fn@c-command.com)<sup>65</sup>. By looking at the messages that SpamSieve missed, we can improve its algorithms to catch such messages in the future.

#### No False Negatives Files

If the **False Negatives** folder is empty, even after enabling **Save false negatives to disk** and training SpamSieve with an uncaught spam message, there is probably a setup problem in your mail program. Use the [Open Log](#) command to see whether SpamSieve made a prediction for that message.

#### Anti-Virus Alerts

It is OK for your anti-virus software to find viruses in the **False Negatives** folder. For more information, see the [Does SpamSieve protect me from viruses?](#) section. If you don't want to see anti-virus alerts, you can either exclude the **False Negatives** folder from scans or uncheck **Save false negatives to disk** and delete all the files in that folder.

### 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 (unless you have **Show recent applications in Dock** checked in the **Dock** pane of System Preferences).

## 6.5 Esoteric Preferences

You can set esoteric SpamSieve preferences by clicking the links on this page. Unlike with regular preferences, you must generally quit and re-launch SpamSieve in order for an esoteric preference to take effect.

#### AddStandardRules

Normally, SpamSieve will [create its standard set](#)<sup>66</sup> of whitelist and blocklist rules if it detects that they are missing. You can also [turn this feature off](#)<sup>67</sup> if you prefer to manage the rules yourself.

#### AppleMailAllJunkMessagesUseBlackText

---

<sup>65</sup><mailto:spamsieve-fn@c-command.com>

<sup>66</sup><x-spamsieve://default?k=AddStandardRules&v=YES>

<sup>67</sup><x-spamsieve://default?k=AddStandardRules&v=NO>

With macOS 10.11 and later, Apple Mail shows messages that its junk filter (or a server filter) thinks are junk using a low-contrast brown/gold/yellow text color. [Click here](#)<sup>68</sup> to have SpamSieve override this and display the messages with the traditional black text color; for the default low-contrast text color [click here](#)<sup>69</sup>.

### AppleMailChangeJunkStatus

Please see the [Faster Apple Mail Training](#) section of the manual.

### AppleMailLaunchSpamSieveSooner

Normally, the Apple Mail plug-in will [launch SpamSieve when Mail launches](#)<sup>70</sup> so that it's ready to filter new messages as soon as they're downloaded. You can also set it to only launch SpamSieve [when it actually starts filtering messages](#)<sup>71</sup>.

### AppleMailPlugInSetIsJunk

Normally, when SpamSieve classifies an incoming message as spam, it tells Apple Mail that the message [is junk](#)<sup>72</sup>. This makes sure that Mail will not display [remote images](#) for that message, thus protecting you from Web bugs. You can also tell SpamSieve [not to](#)<sup>73</sup> mark the messages as junk. This will speed up mail filtering (especially on macOS 10.9), as it will reduce the amount of communication with the mail server.

### AppleMailShowOpenWindow

When SpamSieve's Dock icon is hidden, the Apple Mail plug-in normally adds a **SpamSieve - Open Window** command to Mail's **Message** menu so that SpamSieve's commands are still accessible. If the plug-in is not able to detect that the Dock icon is hidden, you can force it to [show](#)<sup>74</sup> the **Open Window** command or revert back to [auto-detection](#)<sup>75</sup>.

### AppleMailTrainGoodClearFlags

Normally, when you train a message as good in Apple Mail, SpamSieve [preserves any colored flags](#)<sup>76</sup>. If you are using a rule (such as Example 3 in [Spam Message Colors in Apple Mail](#)) to set flags according to spamminess, you can also set SpamSieve to [clear the flags](#)<sup>77</sup> when training a message as good.

### AppleMailTrainGoodGUIScripting/AppleMailTrainSpamGUIScripting

Please see the [Faster Apple Mail Training](#) section of the manual.

### AppleMailTrainGoodGUIScriptingYosemite/AppleMailTrainSpamGUIScriptingYosemite

Please see the [Faster Apple Mail Training](#) section of the manual.

### DisableWhitelistRules

When you train a message as spam, SpamSieve will normally [disable any matching whitelist rules](#)<sup>78</sup> to allow messages like it to be caught as spam. You can also set SpamSieve not to do this, so that [whitelist rules are locked](#)<sup>79</sup> on unless you manually uncheck them.

---

<sup>68</sup>x-spamsieve://default?k=AppleMailAllJunkMessagesUseBlackText&v=YES

<sup>69</sup>x-spamsieve://default?k=AppleMailAllJunkMessagesUseBlackText&v=NO

<sup>70</sup>x-spamsieve://default?k=AppleMailLaunchSpamSieveSooner&v=YES

<sup>71</sup>x-spamsieve://default?k=AppleMailLaunchSpamSieveSooner&v=NO

<sup>72</sup>x-spamsieve://default?k=AppleMailPlugInSetIsJunk&v=YES

<sup>73</sup>x-spamsieve://default?k=AppleMailPlugInSetIsJunk&v=NO

<sup>74</sup>x-spamsieve://default?k=AppleMailShowOpenWindow&v=YES

<sup>75</sup>x-spamsieve://default?k=AppleMailShowOpenWindow&v=NO

<sup>76</sup>x-spamsieve://default?k=AppleMailTrainGoodClearFlags&v=NO

<sup>77</sup>x-spamsieve://default?k=AppleMailTrainGoodClearFlags&v=YES

<sup>78</sup>x-spamsieve://default?k=DisableWhitelistRules&v=YES

<sup>79</sup>x-spamsieve://default?k=DisableWhitelistRules&v=NO

## MJTUpdaterDeleteDiskImage

Normally, the [Software Update...](#) feature will [clean up](#)<sup>80</sup> after itself after downloading a new version. You can also set it to [leave the disk image](#)<sup>81</sup> file in your **Downloads** folder.

## ParseImages

Normally, SpamSieve [analyzes](#)<sup>82</sup> the contents of attached images and PDF files to help detect whether a message is spammy. You can [turn off this feature](#)<sup>83</sup> if you find that corrupt files are confusing macOS's imaging subsystems and leading to crashes.

## QuitMailWhenMacSleeps

As described in the [Why are messages marked as spam in Apple Mail but not moved?](#) section, an OS bug can sometimes cause Mail not to move spam messages out of the inbox if they were received right after the Mac woke from sleep. You can [click here](#)<sup>84</sup> to enable a workaround where SpamSieve quit Mails when the Mac sleeps and relaunches it when the Mac wakes. Or [click here](#)<sup>85</sup> to disable the workaround.

# 7 Frequently Asked Questions (FAQ)

## 7.1 Why is SpamSieve not catching my spam?

SpamSieve is normally highly accurate at filtering out spam messages, and once properly trained it will usually keep working well. If you notice a sudden drop in the filtering accuracy, this is usually because of a problem in your mail program's setup, not because a new type of spam message is evading SpamSieve. (Even if the setup initially worked, it can become incorrect over time due to file corruption or iCloud syncing problems.) This section will help you to fix such setup problems yourself. You can also ask for help if you need additional assistance.

1. When you receive new messages, the mail program needs to send them to SpamSieve for analysis. To make sure that it's set up to do this, find the *Checking the <Mail Client> Setup* section below that corresponds to your mail program and follow the instructions in that section.
2. The mail program will only apply SpamSieve (and your other rules) to messages that *arrive in the Mac's inbox* and are *unread*.
  - Are you reading the messages on a phone or other computer before your Mac sees them?
  - Do you have rules set up on your mail server (or [SaneBox](#)) that move the messages out of the inbox?
  - Is a [server junk filter](#) moving the messages to a **Junk** mailbox?
3. SpamSieve keeps a log of all the messages that it examined and why it thought they were good or spam. The [Open Log](#) section describes how the log can tell you whether a spam message was missed because of the mail program's settings, SpamSieve's settings, or SpamSieve's training.

---

<sup>80</sup>`x-spamsieve://default?k=MJTUpdaterDeleteDiskImage&v=YES`

<sup>81</sup>`x-spamsieve://default?k=MJTUpdaterDeleteDiskImage&v=NO`

<sup>82</sup>`x-spamsieve://default?k=ParseImages&v=YES`

<sup>83</sup>`x-spamsieve://default?k=ParseImages&v=NO`

<sup>84</sup>`x-spamsieve://default?k=QuitMailWhenMacSleeps&v=YES`

<sup>85</sup>`x-spamsieve://default?k=QuitMailWhenMacSleeps&v=NO`

4. The mail program may be having trouble communicating with SpamSieve. To check for communication errors, see the [Sending in an Error Report](#) section.
5. For the best filtering accuracy, SpamSieve needs to be properly trained.
  - The [Checking the Training](#) section has more information about this.
  - Also, make sure that you do not have other rules (besides SpamSieve) in your mail program that move messages to the spam mailbox or trash. Such rules can [prevent you](#) from properly training SpamSieve.
6. You can contact technical support at [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>86</sup>. Before sending your message, please read the [What information should I include when I report a problem?](#) section. Make sure that you've included all of the general information, as well as the items requested in the *If you have spam messages in your inbox* section.

### 7.1.1 Checking the Apple Mail Setup

1. If you do not see the SpamSieve training commands in Mail's **Message** menu, choose **Install Apple Mail Plug-In** from the **SpamSieve** menu. There is more information about this in the [Why don't I see the SpamSieve commands in Apple Mail's Message menu?](#) section.
2. Make sure that SpamSieve has [Full Disk Access](#) and [Automation access](#) to control Mail (if you are using macOS 10.14 or later).
3. Go to the **Junk** pane of Mail's **Preferences** window and make sure that **Enable junk mail filtering** is unchecked.
4. Go to the **Rules** pane of Mail's **Preferences** window and make sure that you have a rule like the one shown in the [Setting Up Apple Mail](#) section:
  - a) Make sure there is a check mark next to the **SpamSieve** rule, indicating that it's active.
  - b) Make sure that the rule's name starts with **SpamSieve**.
  - c) Make sure that the rule's conditions say **Every Message**.
  - d) Make sure that the rule does not have any **Set Color** actions.
  - e) Make sure there are no other rules that move spam messages to another mailbox or the trash. (Exception: in rare cases, you may want to create an "unwanted messages" rule, as described in the [Correct All Mistakes](#) section.)
  - f) Drag the **SpamSieve** rule to the top of the list, if it isn't there already. (Exceptions: If you're using the [drone setup](#), the **Remote Training** rule should be above the **SpamSieve** rule. If you are using an "unwanted messages", as in (e), it should be above the **SpamSieve** rule.)
  - g) Even if the rule looks correct, it can help to delete it and create a new one. (If you do this, be sure to click **Don't Apply** when it asks whether you want to re-apply the rules.)
5. iCloud syncing can cause problems with Apple Mail. If you are not actually using Mail on multiple Macs, you can turn off its iCloud support to prevent these problems. On macOS 10.10 or later, open System Preferences, click on **iCloud**, click the **Options...** button next to **iCloud Drive**, then uncheck **Mail.app**.

---

<sup>86</sup><mailto:spamsieve@c-command.com>

6. If training a spam message in the inbox as spam does not cause it to change color and move to the spam mailbox, please see [Duplicate Apple Mail Accounts](#) section. If you are using macOS 10.14 or later, check that SpamSieve has [Automation access](#) and that you are not using the workarounds for [Faster Apple Mail Training](#).

## Testing That the Rule Works

1. Select a spam message in Mail.
2. Choose **SpamSieve - Train as Spam** from the **Message** menu to tell SpamSieve that it is spam. (If messages don't move to the spam mailbox when trained, please see the [Duplicate Apple Mail Accounts](#) section.)
3. Drag the message to your inbox and select it again.
4. Choose **Apply Rules** from the **Message** menu.  
*Note:* This will also apply your other Mail rules.

If the message moved to the spam mailbox after Step 4, the rule worked. SpamSieve will be able to catch other messages like this if it's properly configured and trained.

If the message did not move to the spam mailbox, there is some other problem with Mail or SpamSieve. Please contact [technical support](#) and explain what happened when you followed these instructions.

### 7.1.2 If the Apple Mail Plug-In Doesn't Appear in the List or Doesn't Stay Enabled

In rare cases, you may not be able to [enable the SpamSieve plug-in in Mail](#) because the plug-in is not listed in the **Manage Plug-ins...** sheet. Or you may click the checkbox to enable it, but it will not stay enabled when you restart Mail.

- A. First, try to uninstall and reinstall the plug-in. Choose [Uninstall Apple Mail Plug-In...](#) from the [SpamSieve menu](#), restart Mail, and then choose [Install Apple Mail Plug-In](#) from the [SpamSieve menu](#). Mail maintains its own separate copy of installed plug-ins, and restarting after uninstalling can get it to clear out its damaged copy, whereas simply installing a fresh copy of the plug-in will not. You may want to temporarily uncheck your SpamSieve rules in Mail's preferences before doing this, so that the uninstaller doesn't offer to delete them, and so that Mail [doesn't move any](#) messages to the **Spam** mailbox while the plug-in is uninstalled.
- B. If that doesn't help, make sure that you have not redirected Mail's plug-ins folder to be stored in a different location. If you haven't tried to move Mail's files or your home folder, you can skip this step. The folder:

`/Users/<username>/Library/Mail/Bundles`

must be stored on the same volume as your home folder (and, ideally, on the boot volume) or Mail will not trust its contents. So you should not try to redirect the whole **Mail** folder to another location, e.g. using a symlink. If you really want your mail to be stored on a different volume, you can move just the **V8** or **V7** folder and replace it with a symlink, or use the Users & Groups preferences pane to move your entire home folder to a different volume.

- C. If you still can't enable the plug-in, or if Mail reports "Incompatible Plug-ins Disabled," the problem may be that Mail's private plug-ins folder is damaged and needs to be reset. Please see the instructions in [Resetting Mail's Private Plug-Ins Folder](#).

### 7.1.3 Resetting Mail's Private Plug-Ins Folder

Sometimes, after you try to [enable the SpamSieve plug-in](#), Mail will report "Incompatible Plug-ins Disabled" (even though the version that you installed *is* compatible) or the installed plug-in will [not appear or not stay checked](#) in the **Manage Plug-ins...** sheet. Such problems generally mean that something is wrong with Mail's *private plug-ins folder*, the place where it stores an extra copy of plug-ins that you have installed *and* enabled in **Manage Plug-ins...** For example, this folder often gets messed up when migrating to a new Mac or restoring from backup.

Since the private plug-ins folder only stores duplicate copies of plug-ins that are also in the public folder (`/Users/<username>/Library/Mail/Bundles/`), you can safely delete the private folder without losing any data, and Mail will then let you enable the plug-in. Please follow the instructions below for the version of macOS that you're using:

#### macOS 11

To delete Mail's private plug-ins folder:

`/Users/<username>/Library/Application Support/Mail/Plug-ins/Bundles/`

1. Quit Mail.
2. Open your user **Library** folder as described in [How can I open the Library folder?](#).
3. Open the **Application Support** folder, then the **Mail** folder, then the **Plug-ins** folder.
4. Drag the **Bundles** folder to the trash. If you can do this, you are done. If macOS won't let you delete the folder, e.g. because it says you don't have permission, you will need to temporarily turn off [System Integrity Protection](#) (as instructed below) so that Mail will let you delete the folder.
5. You may want to print these instructions, write them down, or open them on another computer or device so that you have access to them while rebooting your Mac.
6. Restart your Mac in Recovery Mode. The steps for doing this depend on [which type of processor](#) your Mac has:
  - On an [Intel-based Mac](#), click on the Apple menu and choose **Restart...** Hold down the Command and R keys so that your Mac will reboot in Recovery Mode.
  - On an [Apple Silicon-based Mac](#), click on the Apple menu and choose **Shut Down...** Press and hold the power button on your Mac until you see "Loading startup options." Click **Options**, then click **Continue**, then click **Continue** again.
7. From the **Utilities** menu at the top of the screen, choose **Terminal**.
8. Type `csrutil disable` and press Return. (This is what turns off SIP.)
9. Click on the Apple menu and choose **Restart**.

10. You can now repeat Steps 2–4 to delete the **Bundles** folder.
11. Launch Mail and click on **Manage Plug-ins...** to enable the SpamSieve plug-in.
12. Repeat Steps 6–9, typing `csrutil enable` instead, in order to turn SIP back on.

## macOS 10.15 and Earlier

### *Ask Mail to Reset the DataVaults*

In most cases, asking Mail to reset the **DataVaults** folder will work. To do this:

1. Quit Mail.
2. Open the Terminal app in the **Utilities** folder.
3. Enter this command:

```
defaults delete com.apple.mail EnableBundles
```

and press Return.

4. Launch Mail and then quit it.
5. Enter this command in Terminal:

```
defaults write com.apple.mail EnableBundles -bool YES
```

and press Return.

### *Delete the DataVaults Folder*

If asking Mail to reset the folder doesn't work, you can delete the **DataVaults** folder without losing any important data, and then Mail will recreate it when you try to enable the SpamSieve plug-in, hopefully fixing the problem:

1. You may want to print these instructions, write them down, or open them on another computer or device so that you have access to them while rebooting your Mac.
2. Click on the Apple menu and choose **Restart...** Hold down the Command and R keys so that your Mac will reboot in [Recovery Mode](#). This will enable you to temporarily turn off [System Integrity Protection](#) (as instructed below) so that you have access to delete the protected **DataVaults** folder.
3. From the **Utilities** menu at the top of the screen, choose **Terminal**.
4. Type `csrutil disable` and press Return. (This is what turns off SIP.)
5. Click on the Apple menu and choose **Restart**.
6. The folder:

```
/Users/<username>/Library/Containers/com.apple.mail/Data/DataVaults/
```

needs to be dragged to the trash. (See [How can I open the Library folder?](#) if you have trouble finding it.)

7. Launch Mail and click on **Manage Plug-ins...** to enable the SpamSieve plug-in.
8. You can then repeat Steps 2–5, typing `csrutil enable` instead, in order to turn SIP back on.



#### 7.1.4 If SpamSieve Tells You the Apple Mail Plug-In Isn't Loading, But It Is

If you see the SpamSieve commands in Mail's **Message** menu, that means its plug-in has loaded. In rare cases, SpamSieve may think that the plug-in has not loaded, and ask you to [enable it](#), even though it was actually working properly. For example, this can happen if SpamSieve lacks access to communicate with the plug-in or if Mail takes a very long time to launch.

First, make sure that SpamSieve has [Full Disk Access](#).

If that doesn't fix the problem, please:

1. Click [this link](#)<sup>87</sup> to enable some additional debug logging.
2. If Mail takes a long time to launch, please use Activity Monitor to [record a few samples](#) of it while it's launching. There are also [some tips](#) for how to speed up Mail if it is launching slowly.
3. The next time SpamSieve incorrectly reports that the plug-in has not loaded, please [save a diagnostic report](#) and send it in (along with the sample logs) so that we can investigate what is going wrong on your Mac.

#### 7.1.5 If Apple Mail Doesn't Check for New Messages Automatically

Some macOS 10.13 users have reported that when they are away from a Mac that is either on or in [Power Nap](#), Mail stops downloading new messages from the server, and thus SpamSieve stops cleaning out the inbox. As soon as they sit down at the Mac and unlock the screen, Mail starts processing the messages again. This seems to be caused by a macOS bug that can be worked around by going to **System Preferences** > **Security & Privacy** > **General** and toggling the **Require password** checkbox off and then on again.

#### 7.1.6 If Apple Mail Is Running Slowly

1. In Mail's **Preferences** window, click on the **Accounts** tab, then your account, then the **Server Settings** (formerly **Advanced**) tab, and uncheck **Automatically detect and maintain account settings** (if present).
2. If Mail is launching slowly and you are using macOS 10.14 or later:
  - a) Go to the **Rules** tab of Mail's **Preferences** and uncheck the **SpamSieve** rule.
  - b) Go to the **General** tab of Mail's **Preferences** and click on **Manage Plug-ins...** Uncheck **SpamSieve.mailbundle** and restart Mail.
  - c) Go back to **Manage Plug-ins...** and check **SpamSieve.mailbundle**. Now restart Mail again.
  - d) Go to the **Rules** tab of Mail's **Preferences** and check the **SpamSieve** rule to make it active again.

This should work around a Mail bug where it pauses before loading a plug-in that has been installed for a long time.

---

<sup>87</sup>[x-spamsieve://default?k=InstallerLog&v=YES](#)

3. Change the `AppleMailPlugInSetIsJunk` option in SpamSieve's [esoteric preferences](#) to not mark messages as junk.
4. If training is slow, see the [Faster Apple Mail Training](#) section.
5. If you are using the [Apple Mail - Remote Training](#), [Apple Mail - SaneBox](#), or [Apple Mail - Server Junk Mailbox](#) script, try unchecking the Mail rule that runs the script and see if that helps. You can also run the script in Script Editor to see if it is taking a long time to complete.
6. If none of these suggestions helped, please see the [Sending in a "Sample" Report](#) section.

### 7.1.7 Duplicate Apple Mail Accounts

In rare cases, [two bugs](#) in macOS 10.11 can cause the training commands to fail. The **SpamSieve - Train as Spam** command doesn't move the message to the **Spam** mailbox, and an error such as:

SpamSieve Apple Mail Plug-In [Train as Spam] Error Training: Mail got an error: Can't get mailbox "INBOX" of account "<account>".

is reported in [Console](#). The **SpamSieve - Train as Good** command doesn't move the message to the inbox, and an error such as:

SpamSieve Apple Mail Plug-In [Train as Good] Error Training: Mail got an error: An error of type 8 has occurred.

is reported in [Console](#).

To make the training commands work and prevent these errors:

1. Choose **Preferences** from the **Mail** menu.
2. Click on the **Accounts** tab.
3. Make sure that each account has a unique name. You can edit the **Description** field for an account to change its name so that it is different from the other accounts' names.  
For example, you may have both an active POP account and an inactive IMAP account for the same username and server. These might both be called "Account A". In this case, you could rename the inactive one to "Account A Inactive" so that the names are different.  
If you rename an inactive account, Mail will ask if you want to enable the account. Click **Leave Disabled**.

If renaming the accounts doesn't help, please follow the instructions in the [Sending in an Error Report](#) section.

### 7.1.8 Checking the Airmail Setup

The [Setting Up Airmail](#) section describes how to set up Airmail to filter your mail using SpamSieve.

- The SpamSieve application must be stored *directly* in your **Applications** folder, as shown in the [Installing SpamSieve](#) section.
- Make sure that Airmail has [Automation access](#) to control SpamSieve (if you are using macOS 10.14 or later).

To test that the setup works:

1. When you receive a new message, note its subject.
2. Click on SpamSieve's icon in the Dock.
3. Choose [Open Log](#) from [the SpamSieve menu](#).

The setup is correct if there's a log entry (near the bottom) that says **Predicted: Good** or **Predicted: Spam** and shows the subject for the new message.

If you don't see the expected log entries for new messages:

1. Uncheck **Use SpamSieve** in Airmail's preferences.
2. Quit Airmail, and then launch Airmail.
3. Check **Use SpamSieve** in Airmail's preferences.
4. Repeat the steps above to test whether the setup works.

If you don't see the expected log entries for new messages, please contact [technical support](#) and explain what happened when you followed these instructions.

### Messages Classified as Spam But Not Moved to Spam Mailbox

If you see spam messages in your inbox, it might be because SpamSieve thought they were good, but it might also be that SpamSieve thought they were spam but Airmail was unable to move them to the **Spam** mailbox. To see whether this is the case:

1. Choose [Open Log](#) from [the SpamSieve menu](#). If the log entries for the messages in question say **Predicted: Spam**, that means that SpamSieve did correctly classify them as spam.
2. From Airmail's **Window** menu, choose **Operations**. This will show a log of Airmail's actions, which may provide clues about messages that Airmail tried to move out of the inbox.

#### 7.1.9 Checking the Entourage Setup

1. Choose **Install Entourage Scripts** from the **SpamSieve** menu.
2. Choose **Junk E-mail protection...** from Entourage's **Tools** menu and make sure it's set to **None**.

3. Choose **Mailing List Manager** from Entourage's **Tools** menu. If there are any rules, for each rule click on the **Advanced** tab and make sure that **Do not apply rules to list messages** is unchecked. (If you continue to experience problems, try unchecking each rule itself, to disable it.)
4. Choose **Rules...** from Entourage's **Tools** menu and make sure that you've created two SpamSieve rules, as shown in the [Setting Up Entourage](#) section:
  - a) Make sure that the rules are of the proper type. That is, if you have a POP mail account, you need two POP rules; if you have an IMAP account, you need two IMAP rules.
  - b) Make sure that the **SpamSieve - Move Messages** rule says "if *any* criteria" rather than "if *all* criteria."
  - c) Make sure that the SpamSieve rules are at the top of the list.
  - d) Make sure that the **SpamSieve - Move If Spam** rule is above the **SpamSieve - Move Messages** rule.
  - e) Make sure both SpamSieve rules have check marks next to their names, indicating that they are enabled.
  - f) Make sure there are no other rules that move messages to the **Junk E-mail** folder.

To test that the rules work:

1. Select a spam message in Entourage.
2. Choose **SpamSieve - Train Spam** from the **Scripts** menu to tell SpamSieve that it is spam.
3. Change the category of the message to **None** (using **Edit** > **Categories** > **None**).
4. Choose **Apply Rule** > **SpamSieve - Move If Spam** from the **Message** menu.

If the message's category was changed to **Junk** after Step 4, the rule worked. SpamSieve will be able to catch other messages like this if it's properly configured and trained.

If the message's category did not change to **Junk**, there is some other problem with Entourage or SpamSieve. Please contact [technical support](#) and explain what happened when you followed these instructions.

#### 7.1.10 Checking the GyazMail Setup

1. Make sure that you have followed the instructions in the [Setting Up GyazMail](#) section.
2. Make sure that the **SpamSieve** rule is at the top of the list.
3. If you are using macOS 10.14 or later, make sure that GyazMail has [Automation access](#) to control SpamSieve.

To test that the rules work:

1. Select a spam message in GyazMail.

2. From the **Message** menu, choose **Junk** ▸ **Mark as Junk**.
3. Drag the message back to your inbox and select it there.
4. From the **Message** menu, choose **Apply Rule** ▸ **All Rules**.

If the message moves back to your spam mailbox, the rule worked. SpamSieve will be able to catch other messages like this if it's properly configured and trained.

Otherwise, there is some other problem with GyzMail or SpamSieve. Please contact [technical support](#) and explain what happened when you followed these instructions.

#### 7.1.11 Checking the MailMate Setup

1. Make sure that you have followed the instructions in the [Setting Up MailMate](#) section.
2. If you are using macOS 10.14 or later, make sure that MailMate has [Automation access](#) to control SpamSieve.

To test that the setup works:

1. When you receive a new message, note its subject.
2. Click on SpamSieve's icon in the Dock.
3. Choose [Open Log](#) from [the SpamSieve menu](#).

The setup is correct if there's a log entry (near the bottom) that says **Predicted: Good** or **Predicted: Spam** and shows the subject for the new message.

If you don't see the expected log entries for new messages, please contact [technical support](#) and explain what happened when you followed these instructions.

#### 7.1.12 Checking the Mailsmith Setup

The [Setting Up Mailsmith](#) section describes how to set up Mailsmith to filter your mail using SpamSieve.

1. Make sure that you are using version 2.3.1 or later of Mailsmith.
2. Make sure that **Use SpamSieve** is checked in the preferences. If that option is disabled:
  - a) Make sure you have only one copy each of Mailsmith and SpamSieve installed. If there are any old versions in the trash, empty the trash.
  - b) Launch SpamSieve directly from the Finder, by double-clicking its icon. (Do not use the Dock icon or an application launcher.)
  - c) Launch Mailsmith (again, by double-clicking its icon).
  - d) Open Mailsmith's **Preferences** window, and verify that the **Use SpamSieve** option is enabled.

3. If you are using the **Leave it in “(incoming mail)”** option, make sure that a deposit or transfer filter isn’t acting on the spam messages before your spam filter can.
4. To test the connection between Mailsmith and SpamSieve, select a message and choose **Recalculate Spam Score** from Mailsmith’s **Message** menu. Then choose [Open Log](#) in SpamSieve and verify that a “Predicted” entry for that message was added to the log.

### 7.1.13 Checking the Outlook 2011 Setup

1. Make sure that Outlook has [Automation access](#) to control SpamSieve (if you are using macOS 10.14 or later).
2. Choose **Install Outlook Scripts** from the **SpamSieve** menu.
3. Choose **Junk E-mail protection...** from Outlook’s **Tools** menu and make sure it’s set to **None**.
4. Choose **Mailing List Manager...** from Outlook’s **Tools** menu. If there are any rules, for each rule click on the **Advanced** tab and make sure that **Do not apply rules to list messages** is unchecked. (If you continue to experience problems, try unchecking each rule itself, to disable it.)
5. Choose **Rules...** from Outlook’s **Tools** menu and make sure that you’ve created two SpamSieve rules, as shown in the [Setting Up Outlook 2011](#) section:
  - a) Make sure that the rules are of the proper type. That is, if you have a POP mail account, you need two POP rules; if you have an IMAP account, you need two IMAP rules.
  - b) Make sure that the **SpamSieve - Move Messages** rule says “If *any* conditions” rather than “If *all* conditions.”
  - c) Make sure that the SpamSieve rules are at the top of the list.
  - d) Make sure that the **SpamSieve - Set Category** rule is above the **SpamSieve - Move Messages** rule.
  - e) Make sure both SpamSieve rules have check marks next to their names, indicating that they are enabled.
  - f) Make sure there are no other rules that move messages to the **Junk E-mail** folder.
6. Choose **Accounts...** from Outlook’s **Tools** menu. If you have any IMAP accounts, click the **Advanced...** button, then click the **Folders** tab, and make sure that it’s set to **Move deleted message to this folder**. Otherwise, the caught spams may still appear on your iPhone.
7. Choose **Preferences...** from the **Outlook** menu and click on **Reading**. Make sure that **Hide IMAP messages marked for deletion** is checked. This will ensure that you do not see spam messages that were caught on another computer.

To test that the rules work:

1. Select a spam message in Outlook.
2. Choose **SpamSieve - Train as Spam** from the **Scripts** menu to tell SpamSieve that it is spam.
3. Remove the categories of the message (using **Message ▸ Categorize ▸ Clear All**).

4. Drag the message back to your inbox and select it there.
5. Choose **Rules > Apply > SpamSieve - Set Category** from the **Message** menu.

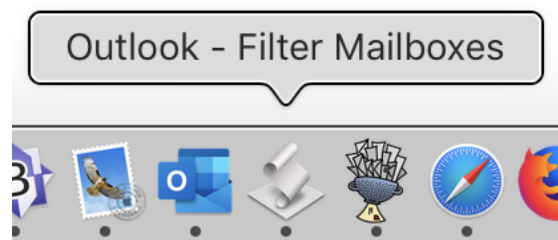
If the message's category was changed to **Junk** after Step 5, the rule worked. SpamSieve will be able to catch other messages like this if it's properly configured and trained.

If the message's category did not change to **Junk**, there is some other problem with Outlook or SpamSieve. Please contact [technical support](#) and explain what happened when you followed these instructions.

#### 7.1.14 Checking the Outlook Setup

These instructions apply to Microsoft Office 365 (also known as Outlook 2016 and Outlook 2019, versions 15.x and 16.x). For other versions of Outlook, please see the [Checking the Outlook 2011 Setup](#) section.

1. Make sure that the **Outlook - Filter Mailboxes** app is running in your Dock, as described in Step 5 of the [Setting Up Outlook](#) section.



*Note:* If it was already running, it may help to quit and relaunch it.

2. If you are using macOS 10.14 or later, make sure that **Outlook Filter Mailboxes** has [Automation access](#) to control Outlook and SpamSieve. **Script Menu** or **FastScripts** (depending on which you are using) also needs **Automation** access to control Outlook and SpamSieve.
3. Choose **Install Outlook Scripts** from the **SpamSieve** menu.
4. Select a spam message in Outlook.
5. Choose **SpamSieve - Train as Spam** from the **Scripts** menu to tell SpamSieve that it is spam.
6. Remove the categories of the message (using **Message > Categorize > Clear All**).
7. Drag the message back to your inbox and select it there.
8. Choose **SpamSieve - Move If Spam** from the **Scripts** menu.

If the message moved to the **Junk E-mail** folder and its category was changed to **Junk** after Step 7, the script worked. SpamSieve will be able to catch other messages like this if it's properly configured and trained.

If the message's category did not change to **Junk**, there is some other problem with Outlook or SpamSieve. Please contact [technical support](#) and explain what happened when you followed these instructions. Please include your [Console log](#). There are also links on the [script page](#) to enable debug logging so that additional information is logged.

### 7.1.15 Checking the Postbox Setup

The [Setting Up Postbox](#) section describes how to set up Postbox to filter your mail using SpamSieve.

1. Go to Postbox's **Tools** menu and choose **Add-ons**. The **Installed Add-Ons** section of the window should show **SpamSieve Postbox Plug-in**.
2. Make sure that **Do not mark mail as junk if the sender is in...** is not checked.
3. Make sure that **Trust junk mail headers set by...** is not checked.

To test that the setup works:

1. When you receive a new message, note its subject.
2. Click on SpamSieve's icon in the Dock.
3. Choose **Open Log** from the **SpamSieve** menu.

The setup is correct if there's a log entry (near the bottom) that says **Predicted: Good** or **Predicted: Spam** and shows the subject for the new message.

If you don't see the expected log entries for new messages, please contact [technical support](#) and explain what happened when you followed these instructions.

### 7.1.16 Checking the PowerMail Setup

1. Quit PowerMail, delete the folder:

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

and then re-launch PowerMail. (See the [How can I open the Library folder?](#) section.) If the script files that PowerMail uses to communicate with SpamSieve are damaged, this will fix them.

2. Make sure that you've followed the instructions in the [Setting Up PowerMail](#) section.
  - Make sure that the conditions for the **Spam: evaluate** filter are not excluding the messages that you want SpamSieve to filter. For example, try editing the filter so that it has just a single condition that says **Always**.
  - Make sure that the **Spam: evaluate** filter is at the top of the list.
  - Make sure that the **Spam: actions** filter is directly below the **Spam: evaluate** filter.

To test that the setup works:

1. Select a spam message in PowerMail.
2. Choose **Mark as Spam** from the **Mail** menu to tell SpamSieve that it is spam.
3. Choose **Perform Filter** > **Spam: evaluate** from the **Mail** menu.



4. Click on SpamSieve's icon in the Dock. Then choose **Open Log** from the **SpamSieve** menu.

The setup is correct if the last entry in the log says **Predicted:** **Spam** and shows the subject for the message that you had selected. SpamSieve will be able to catch other messages like this if it's properly configured and trained.

Otherwise, there is some other problem with PowerMail or SpamSieve. Please contact [technical support](#) and explain what happened when you followed these instructions.

### 7.1.17 Checking the Training

SpamSieve is nearly 100% accurate, but only when properly trained. Here's how you can check the training:

1. Choose **Show Statistics** from the **Filter** menu. Does the **Corpus** section show at least 100 spam messages and 100 good messages? If not, follow the instructions in the [Do an Initial Training](#) section.
2. If SpamSieve has misclassified any messages, it needs to know this or its accuracy will decline. This is described in the [Correct All Mistakes](#) section. If SpamSieve misclassified some messages and you have not yet corrected its mistakes, do so now. If you've already deleted the misclassified messages, it's too late to correct the mistakes; choose **Reset Corpus** from the **Filter** menu and then follow the instructions in the [Do an Initial Training](#) section.
3. Check the percentage of spam messages in the **Corpus** section of the **Statistics** window. It should be between 55% and 75%. If not, train SpamSieve with more spam or good messages so that the percentage is in this range.
4. Check the number of spam and good messages in the **Corpus** section of the **Statistics** window. If the corpus is very large (more than 4,000 messages) *and* SpamSieve is not catching your spam, the corpus may contain incorrect or obsolete messages that reduce SpamSieve's effectiveness and make it slower to adapt. Choose **Reset Corpus** from the **Filter** menu and then follow the instructions in the [Do an Initial Training](#) section.

*Note:* You should only reset the corpus after you've [checked](#) all the other items in the [Why is SpamSieve not catching my spam?](#) section.

### 7.1.18 How do I make SpamSieve catch spams sent from my own address?

Sometimes spammers forge one of your e-mail addresses and send you spam messages that appear to be coming from yourself. If SpamSieve is not properly configured, these spams will keep coming into your inbox even after you train them as spam. (Yes, you [should](#) train them as spam if they get through to your inbox.) Once you fix the configuration, SpamSieve will be able to catch these messages as easily as any other spams.

#### Why does SpamSieve let these obvious spams into my inbox?

SpamSieve does what you tell it to do. Under the standard configuration, the [Use macOS Contacts](#) option is enabled in SpamSieve's preferences. This is safety feature so that messages from people in your address book are never marked as spam. If your address is in the address book and a spammer sends a message from that address, SpamSieve will let it through to your inbox. It will do this no matter how blatantly spammy the message is; doing otherwise would counteract the safety feature.

## How can I tell whether I need to fix the setup?

The [Open Log](#) section of the manual explains how SpamSieve keeps a log of all the messages that it filtered and why it thought they were good or spam. For each incoming message that SpamSieve thought was not spam, there is a **Predicted: Good** entry in the log. If it says **Reason: sender <address> in address book** or **Reason: sender <address> in Entourage address book**, that means that SpamSieve thought the message was good because it was sent from an address that's in your address book. If the address is one of your addresses, please follow the instructions below. (If there's no **Predicted** entry for the message, please see the [Why is SpamSieve not catching my spam?](#) section for instructions on checking the setup in your mail program.)

## How do I make SpamSieve catch these spams?

SpamSieve has a feature specifically for catching this kind of spam. For messages sent from your address, SpamSieve will ignore the fact that your own address is in your address book. It will apply its normal Bayesian filtering engine to examine the entire contents of the message and evaluate whether it is spam. To use this feature, you need to do two things:

1. Make sure that [Exclude my addresses](#) is checked in SpamSieve's preferences. This tells SpamSieve to pretend that your address is not in the address book, thus bypassing the [Use macOS Contacts](#) safety feature (but only for messages sent from one of your own addresses).
2. Tell SpamSieve which addresses are yours. You do this by listing them on your card in the Contacts (previously Address Book) application.

If the addresses are already entered in your e-mail program's preferences, you can quickly add them by choosing [Update Address Book "Me" Card](#) from the **SpamSieve** menu. If you have other addresses, you'll need to add them manually from the Contacts application. Add the addresses to your card, making sure to enter them in the e-mail address section rather than the phone number section.

Your card is the one that has your name and photo (or login image). It says "me" on top of the photo, and in the name list it has a black silhouette of a head and shoulders instead of a white address book card. To find your "me" card, choose **Card ▸ Go to My Card**. If you don't have a "me" card, you can make one by creating a new card with your name and addresses and choosing **Card ▸ Make This My Card**.

## 7.2 What information should I include when I report a problem?

It will be faster and easier to help you if your e-mail includes all of the following information:

### The version of macOS that you are using

Click on the Apple menu and choose **About This Mac**.

### The version of SpamSieve that you are using

Click on the SpamSieve menu and choose **About SpamSieve**. (Please do not say "the latest version," as this is ambiguous.)

### The name and version of your e-mail program

In your mail program, click on the application menu and choose **About <Mail Program Name>**. (If you're using Apple Mail, it's not necessary to specify the version.)

### Information about your e-mail setup

- Do you access your e-mail from multiple computers? If so, on how many of them is SpamSieve installed?
- If you are using SpamSieve with the same e-mail account on multiple Macs, which one of the [four approved setups](#) are you using?
- Do you access your e-mail from a mobile device such as an iPhone, iPad, iPod, or BlackBerry?
- Are you using SpamSieve with multiple e-mail accounts? If so, does the problem pertain to all of them?

#### **If you have uncaught spam messages**

- Are the uncaught spam messages in your inbox or in another folder?
- When you first saw the uncaught spam messages on your Mac, were they marked as read or unread?
- Please *do not forward the problem messages* using your mail program. Instead, make a new e-mail to [spamsieve-fn@c-command.com](mailto:spamsieve-fn@c-command.com)<sup>88</sup> and include SpamSieve’s log file as an attachment (see [Sending in the SpamSieve Log File](#)).
- Depending on the situation, we may ask you to send in any applicable false negatives files (see [Sending in False Negative Files](#)).

#### **If you have good messages in your Spam mailbox**

- What are the sender address and subject for each good message that you’re referring to?
- Please *do not forward the problem messages* using your mail program. Instead, make a new e-mail to [spamsieve-fn@c-command.com](mailto:spamsieve-fn@c-command.com)<sup>89</sup> and include SpamSieve’s log file as an attachment (see [Sending in the SpamSieve Log File](#)).

#### **If it will help you explain what’s happening or what you are seeing**

Please see [Sending in Screenshots](#).

#### **If something aside from SpamSieve’s filtering is not working properly**

Please see [Sending in an Error Report](#).

#### **If SpamSieve or the mail program hangs, freezes, or is very slow**

Please see [Sending in a “Sample” Report](#).

#### **If the mail program crashes**

Please see [Sending in Crash Log Files](#) and [What can I do if Apple Mail is crashing?](#).

For other types of problems, please describe what you did, what happened, and what did you expect to happen instead. This will make it easier for us to understand the issue that you are reporting.

### **7.2.1 Sending in an Error Report**

If an error window appeared on your screen, please include the exact text of the error message in your e-mail. (It may help to use **Copy** and **Paste**.)

Please also send in any errors that were reported in the system log:

---

<sup>88</sup><mailto:spamsieve-fn@c-command.com>

<sup>89</sup><mailto:spamsieve-fn@c-command.com>

1. From SpamSieve's **Help** menu, choose **Save Diagnostic Report...** at the bottom. (If you can't access the **Help** menu because the Dock icon is hidden, click [this link](#)<sup>90</sup> to save a diagnostic report. If you can't launch SpamSieve to access its **Help** menu, see below.)
2. Choose a location such as your desktop and click **Save**. Saving the report may take a minute or so.
3. Create an e-mail to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>91</sup> and drag the **Diagnostic Report.tbz** file into the e-mail message to include it as an attachment/enclosure.

If you can't launch SpamSieve, you can access the log directly, rather than using the automated diagnostic reporter:

### macOS 10.12 and Later

1. Click on Finder in the Dock.
2. From the **Go** menu, choose **Utilities**.
3. Double-click the Console application.
4. Click on your Mac under **Devices** at the left side of the window. (It may be necessary to first choose **Show Sources** from the **View** menu.)
5. From the **Action** menu, choose **All Messages**. Make sure that **Include Info Messages** and **Include Debug Messages** are both unchecked.
6. If **Activities** is selected (blue) in the toolbar, click it to turn off activities mode.
7. If the main part of the window shows any recent error messages, select them (or choose **Edit** ▸ **Select All**).
8. There are two ways to share the selected part of the log with us:
  - *Easier*: Click the **Share** button in the toolbar and choose **Mail**. (If you do not use Apple Mail as your mail client, you can instead **Copy** and **Paste** the log messages into your mail client.)
  - *Preferred*: Choose **Edit** ▸ **Copy**. Open TextEdit and **Paste** the text into a new plain text document. Save the TextEdit document to disk and attach it to your e-mail message.

### macOS 10.11 and Earlier

1. Click on Finder in the Dock.
2. From the **Go** menu, choose **Utilities**.
3. Double-click the Console application.
4. Click on **All Messages** at the left of the window. (It may be necessary to first click the **Show Log List** toolbar button if you don't see **All Messages** at the left.)

---

<sup>90</sup>`x-spamsieve://diagnosticReport`

<sup>91</sup>`mailto:spamsieve@c-command.com`

5. If it shows any recent error messages, select them (or choose **Edit** ▸ **Select All**).  
*Note:* You may need to click the **Earlier** button at the bottom of the window to find errors that did not occur recently.
6. Choose **File** ▸ **Save Selection As...** and save the file as **My Log.log** on your desktop.
7. Drag this file into your e-mail message to include it as an attachment/enclosure.

### 7.2.2 Sending in the SpamSieve Log File

SpamSieve's [log file](#) contains information about the incoming messages that it has processed as well as the messages that you've trained it with. If SpamSieve is not behaving the way that you expect, the log file can help pinpoint the source of the problem.

To send in the log file:

1. From SpamSieve's **Help** menu, choose **Save Diagnostic Report...** at the bottom. (If you can't access the **Help** menu because the Dock icon is hidden, click [this link](#)<sup>92</sup> to save a diagnostic report. If you can't launch SpamSieve to access its **Help** menu, see below.)
2. Choose a location such as your desktop and click **Save**. Saving the report may take a minute or so.
3. Create an e-mail to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>93</sup> and drag the **Diagnostic Report.tbz** file into the e-mail message to include it as an attachment/enclosure.

If you can't launch SpamSieve, you can access the log directly, rather than using the automated diagnostic reporter. The log file is stored at:

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

You cannot find the log file by searching your Mac because Spotlight does not index the folder the contains it. Instead, you can find the log file by following these instructions:

1. Open your user **Library** folder, as described in the [How can I open the Library folder?](#) section.
2. Inside the **Library** folder, open the **Logs** folder.
3. Inside the **Logs** folder, open the **SpamSieve** folder.
4. Inside the **SpamSieve** folder, find the **SpamSieve Log.log** file.  
*Note:* In most cases, you can ignore old, dated log files, whose names end with **.log.bz2**. Just send the **SpamSieve Log.log** file.
5. Drag the **SpamSieve Log.log** file into the message window in your e-mail program to attach it to your message. The file should be included as an attachment/enclosure, not as text in the body of the message.

---

<sup>92</sup>`x-spamsieve://diagnosticReport`

<sup>93</sup>`mailto:spamsieve@c-command.com`

### 7.2.3 Sending in Screenshots

To help troubleshoot problems in your mail program, please include screenshots of:

1. Any errors that were reported (if applicable).
2. The message list in your mail program.
3. The rule list in your mail program (including both regular rules and mailing list manager rules, if applicable).
4. The individual SpamSieve rule(s) that you created in the mail program.

To take a screenshot, hold down the Command 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 **Screen Shot <date> at <time>.png** on your desktop. Pressing the keys again will create **Screen Shot <date> at <new time>.png**, etc.

You can also take screenshots using the **File > Take Screenshot** command in the Preview application.

To send in screenshots, drag the files into your e-mail window to attach them to your message. If you're using Apple Mail, be sure to set the **Image Size** pop-up menu at the bottom of the message window to **Actual Size**.

### 7.2.4 Sending in False Negative Files

In the **Advanced** tab of SpamSieve's **Preferences** window, make sure that [Save false negatives to disk](#) is checked. When you train a message as spam that SpamSieve thought was good, it will save that message as a file. Click the **Show** button in the **Preferences** window to open the folder. You can then drag the folder (or particular files in it) into the message window in your e-mail program. You can use Quick Look to view the message files to help find the ones that you want.

If a spam message gets through and is *not* saved in the **False Negatives** folder, this likely means that there is a setup problem and that SpamSieve was not given an opportunity to filter that message. Please see the [Why is SpamSieve not catching my spam?](#) page for information about how to fix setup problems.

### 7.2.5 Sending in a “Sample” Report

If a program is slow, hangs (e.g. with a spinning beachball), or freezes, a “sample” report can record what your Mac was doing in order to locate the source of the problem.

1. Click on Finder in the Dock.
2. From the **Go** menu, choose **Utilities**.
3. Double-click the Activity Monitor program.
4. Select SpamSieve in the **Activity Monitor** window.

5. Do whatever it is in SpamSieve that causes the slowness, hang, or freeze. *Immediately*, click on Activity Monitor in the Dock and choose **Sample Process** from the **View** menu.
6. After Activity Monitor has finished taking the sample, click the **Save...** button in the “Sample of SpamSieve” window. Save the file to your desktop and then include it in your e-mail message to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>94</sup> as an attachment. (Please do not copy and paste the text from the Activity Monitor window.)

(If you aren’t sure whether the problem pertains to SpamSieve or the mail program, please repeat steps 4–6 for both SpamSieve and the mail program.)

### 7.2.6 Sending in Crash Log Files

If SpamSieve itself crashes, the **SpamSieve Crash Reporter** window should automatically come up. Make sure that you enter a valid e-mail address and then click the **Send Report** button.

If your mail program (or a helper process such as `spamsieve-reader`) crashes, you’ll need to send in the crash log file manually.

Crash logs are stored in the folder:

```
/Users/<username>/Library/Logs/DiagnosticReports/
```

First click on the Finder in the Dock, then click on the **Go** menu, and hold down the Option key as you choose **Library**. Open the Logs folder, then DiagnosticReports.

Once you’ve opened the DiagnosticReports folder, find the most recent crash log file for the app that crashed and add it to your e-mail message to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>95</sup> as an attachment.

*Note:* You may be able to temporarily stop crashes in Apple Mail by removing all of the `.mailbundle` files from the folder:

```
/Users/<username>/Library/Mail/Bundles/
```

### 7.2.7 Sending in Apple Mail Rules

If there is a problem setting up your rules in Mail, or if the rules don’t work as you expect, please send in the rules file(s).

1. From SpamSieve’s **Help** menu, choose **Save Diagnostic Report...** at the bottom. (If you can’t access the **Help** menu because the Dock icon is hidden, click [this link](#)<sup>96</sup> to save a diagnostic report. If you can’t launch SpamSieve to access its **Help** menu, see below.)
2. Choose a location such as your desktop and click **Save**. Saving the report may take a minute or so.

---

<sup>94</sup><mailto:spamsieve@c-command.com>

<sup>95</sup><mailto:spamsieve@c-command.com>

<sup>96</sup>`x-spamsieve://diagnosticReport`

3. Create an e-mail to [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>97</sup> and drag the `Diagnostic Report.tbz` file into the e-mail message to include it as an attachment/enclosure.

If you can't launch SpamSieve, you can access the rules files directly, rather than using the automated diagnostic reporter:

- On macOS 10.12, the files are stored at:

```
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V4/MailData/RulesActiveState.plist
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V4/MailData/SyncedRules.plist
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V4/MailData/UnsyncedRules.plist
```

1. Click on the Finder in the Dock.
2. Click on the **Go** menu at the top of the screen, hold down the Option key, and then choose **Library**.
3. Open the **Containers** folder, then **com.apple.mail**, then **Data**, then **Library**, then **Mail**, then **V4**, then **MailData** to find the **RulesActiveState.plist**, **SyncedRules.plist**, and **UnsyncedRules.plist** files.

- On macOS 10.11, the files are stored at:

```
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V3/MailData/RulesActiveState.plist
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V3/MailData/SyncedRules.plist
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V3/MailData/UnsyncedRules.plist
```

1. Click on the Finder in the Dock.
2. Click on the **Go** menu at the top of the screen, hold down the Option key, and then choose **Library**.
3. Open the **Containers** folder, then **com.apple.mail**, then **Data**, then **Library**, then **Mail**, then **V3**, then **MailData** to find the **RulesActiveState.plist**, **SyncedRules.plist**, and **UnsyncedRules.plist** files.

- On macOS 10.8 through 10.10, the files are stored at:

```
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V2/MailData/RulesActiveState.plist
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V2/MailData/SyncedRules.plist
/Users/<username>/Library/Containers/com.apple.mail/Data/Library/Mail/V2/MailData/UnsyncedRules.plist
```

1. Click on the Finder in the Dock.
2. Click on the **Go** menu at the top of the screen, hold down the Option key, and then choose **Library**.
3. Open the **Containers** folder, then **com.apple.mail**, then **Data**, then **Library**, then **Mail**, then **V2**, then **MailData** to find the **RulesActiveState.plist**, **SyncedRules.plist**, and **UnsyncedRules.plist** files.

---

<sup>97</sup><mailto:spamsieve@c-command.com>



### 7.3 Why is every message going to the Spam mailbox?

It is unlikely that SpamSieve is mistakenly thinking that *all* your mail is spam. To see whether the messages are going to the **Spam** mailbox because of SpamSieve, you can use the [Open Log](#) command.

More likely, the messages are being moved by a mail program on another computer, by a [server](#) filter, or by a problem with your mail program, as described below:

#### Apple Mail

1. If SpamSieve's plug-in is not installed or not [enabled](#) (e.g. if it was disabled by an OS update), Mail will move every message to the **Spam** mailbox without consulting SpamSieve. To re-install the plug-in, choose [Install Apple Mail Plug-In](#) from the **SpamSieve** menu. When the plug-in is properly installed and loaded, you will see the training commands in Mail's **Message** menu. See also the [Why don't I see the SpamSieve commands in Apple Mail's Message menu?](#) section.
2. Make sure that you've disabled Mail's built-in junk mail filter, as described in Step 7 of the [Setting Up Apple Mail](#) section.
3. Make sure that the only spam/junk rule that you have in Mail's preferences is **SpamSieve**.
4. The name of the SpamSieve 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.
5. To separate the good messages in the **Spam** mailbox from the spam ones, drag all the unread messages to the inbox. Then select them and choose **Apply Rules** from the **Message** menu. (You can alternatively use the [Apple Mail - Move If Spam script](#) with the `moveGoodMessagesToInbox` option.)

#### Entourage

1. Make sure that you've disabled Entourage's built-in Junk Mail Filter.
2. Make sure that the SpamSieve rule in Entourage are set up [exactly as shown](#).
3. Make sure that the only spam/junk rules that you have in the **Rules** window are the two SpamSieve rules.

#### Outlook 2011

1. Make sure that you've disabled Outlook's built-in Junk Mail Filter.
2. Make sure that the SpamSieve rule in Outlook are set up [exactly as shown](#).
3. Make sure that the only spam/junk rules that you have in the **Rules** window are the SpamSieve rules.

## 7.4 Why do good messages keep going to the Junk or Spam mailbox?

Normally, as soon as you train one message as good, SpamSieve will add the message's sender to its [whitelist](#). This means that SpamSieve will never classify future messages from that sender as spam. Also, by default, SpamSieve will never classify messages [from senders in your contacts](#) as spam. Nevertheless, there are several reasons why such messages might keep ending up in the **Junk** or **Spam** mailbox:

1. A junk filter on the server might be classifying the messages as spam. This is especially likely to be the case if the messages are going to a [different mailbox](#) than the one that SpamSieve uses. In many cases, there is no visible switch to turn a server filter on/off, so it will be on unless you create a specific rule to turn it off. Please see the [How should I configure the junk filter on my mail server?](#) section.
2. Regardless of whether SpamSieve thinks a message is spam, the message can still end up in the **Spam** mailbox if you have created other rules in your mail client that move messages to the **Spam** mailbox. It is recommended that you disable or delete such rules. Also make sure that your mail client's built-in junk filter is off. To help isolate what SpamSieve itself is doing, you can create a separate spam mailbox called **SpamSieve Spam** and edit your mail program's SpamSieve rule to use that mailbox.
3. Another computer that accesses your mail account may have rules or a spam filter that are moving the messages. You can narrow down which one is responsible by temporarily setting each server filter or copy of SpamSieve to use a different **Spam** mailbox. For example, set the copy of SpamSieve on your MacBook [to use a mailbox called SpamSieveMacBook](#).
4. Your mail client may be moving all incoming messages to the spam mailbox because of a setup problem. Please see the [Why is every message going to the Spam mailbox?](#) section.
5. SpamSieve might have classified the message as spam. You can see whether it has done this by using the [Open Log](#) command and looking for a **Predicted: Spam** entry for the message.

How could this happen when you had trained similar messages as good? If you train a message as good and then subsequently train a message from that same sender as spam, SpamSieve will disable the whitelist rule and add a rule to the [blocklist](#). Then SpamSieve will classify messages from that sender as spam until you train another one as good. At that point, there will be rules on both the whitelist and the blocklist, both disabled, so SpamSieve will determine whether messages are spam by looking at their complete contents. If you don't want it to do this, but to instead treat all the messages from that sender as good, you can add the sender to your address book or find the sender's rule in the **Whitelist** window and click the checkbox to re-enable it.

You can contact technical support at [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>98</sup>. Before sending your message, please read the [What information should I include when I report a problem?](#) section. Make sure that you've included all of the general information, as well as the items requested in the *If you have good messages in your Spam mailbox* section.

## 7.5 Can I delete spam messages that are in the spam folder?

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.

---

<sup>98</sup><mailto:spamsieve@c-command.com>

Before you delete any messages, make sure that you have [corrected all the mistakes](#). To make it easier to find any good messages that are accidentally in the **Spam** mailbox, you may find it helpful to sort by subject or to [separate the spam messages by color](#).

To manually delete old spam messages, you can simply select them in your mail program (using **Edit** > **Select All** may help) and press the Delete key.

To automatically delete old spam messages, please see the [Automatically Deleting Old Spam Messages](#) page.

## 7.6 How should I configure the junk filter on my mail server?

### Spam in Other Locations

SpamSieve moves the spam messages that arrive in your inbox into a separate mailbox, usually called **Spam**. When you train a message as spam, SpamSieve also puts it in that mailbox.

You may find that you have a second **Spam** mailbox or a **Junk** mailbox that is also filling up with spam. These spams were likely caught by a junk filter on your mail server. The server filter catches its spam messages before the Mac sees them, so:

- It is normal for some spams to be in the server's spam mailbox rather than SpamSieve's. SpamSieve never had a chance to process these messages, so they are not mistakes. You should not train them as spam.
- It is normal for there to be some good messages in the server's spam mailbox. These are also not SpamSieve mistakes, since the server filter put them there without SpamSieve seeing them. You should not train them as good.

The [Consolidating Spam From Multiple Filters](#) section describes some ways to handle spam messages in multiple locations.

### SpamSieve vs. Server Filters

SpamSieve is compatible with junk/spam filters that run on the mail server, however we recommend that most users turn them off because:

- In most cases, SpamSieve will catch the same spam messages (and more), so the server spam filter is not providing much benefit. Exception: If your Mac and SpamSieve will often be off or disconnected from the Internet, the server spam filter can help keep spam off your iPhone during that time.
- Server spam filters are [more likely](#) to mistakenly classify your good messages as spam. Because the server filters the messages before they get to your Mac, SpamSieve cannot “save” you from these mistakes. In some cases, these good messages may be deleted sight-unseen or “lost,” only visible when you log into a special spam quarantine mailbox via a Web browser.
- Server spam filters often move suspected spam messages to a special mailbox, which is separate from your other accounts and from SpamSieve's **Spam** mailbox. (See “Spam in Other Locations” above.) Most users find it simplest to review a single spam mailbox for all their accounts.

### Turning Off Your Server-Side Spam Filter

Please find the “Turning Off” section below that corresponds to your mail provider. Note that some mail hosts, such as Media Temple, have both per-account and per-user spam filters, so there may be more than one switch to turn off. If your mail provider does not let you turn off its spam filter, we recommend switching to one of the [Recommended Mail Hosts](#).

### Re-filtering Messages Caught by the Server Filter

You can use the [Apple Mail - Server Junk Mailbox](#) script to have SpamSieve save you from mistakes that the server junk filter made by moving any messages that it thinks are good back to the inbox. It will also [consolidate](#) the spam messages from all the accounts into a single spam mailbox (the same one where SpamSieve is already putting your spam).

### Bulk Mail and Quarantine

Some mail providers have a mailbox called **Bulk Mail** or a special Web site to view messages that are “quarantined.” If possible, we recommend turning off these features for the same reasons described above. Regardless, there are two important points to keep in mind:

- The server puts the messages in the bulk mailbox before SpamSieve sees them. Thus, there is no setting you can change in SpamSieve to prevent this from happening.
- Since these messages are invisible to SpamSieve, it is not necessary or recommended that you train it with them.

If you cannot turn off your server’s **Bulk Mail** mailbox, you can use the [Apple Mail - Server Junk Mailbox](#) script to have SpamSieve sort through the bulk mail for you.

#### 7.6.1 Turning Off the AOL Spam Filter

It no longer seems to be possible to turn off the AOL spam filter. Please see the alternative options in the [Consolidating Spam From Multiple Filters](#) section of the manual. For example, you can set up SpamSieve to rescue good messages caught by AOL’s junk filter and move the spam messages to SpamSieve’s mailbox.

#### 7.6.2 Turning Off the Fastmail Spam Filter

1. Log into [Fastmail’s Web mail](#) and click on the **Mail** menu at the top left.
2. Click on **Settings**, then **Spam Protection**.
3. Make sure that **Custom** is selected:

## Spam Protection

We give each message a score for how suspicious it appears.

Protection level:

☐ Off

☐ Standard

☐ Aggressive

☒ Custom

✓ **Reject** messages from insecure servers

☐ **Move** messages with a score of  or higher to **Spam**

☐ **Permanently delete** messages with a score of  or higher

☐ Mark spam as read

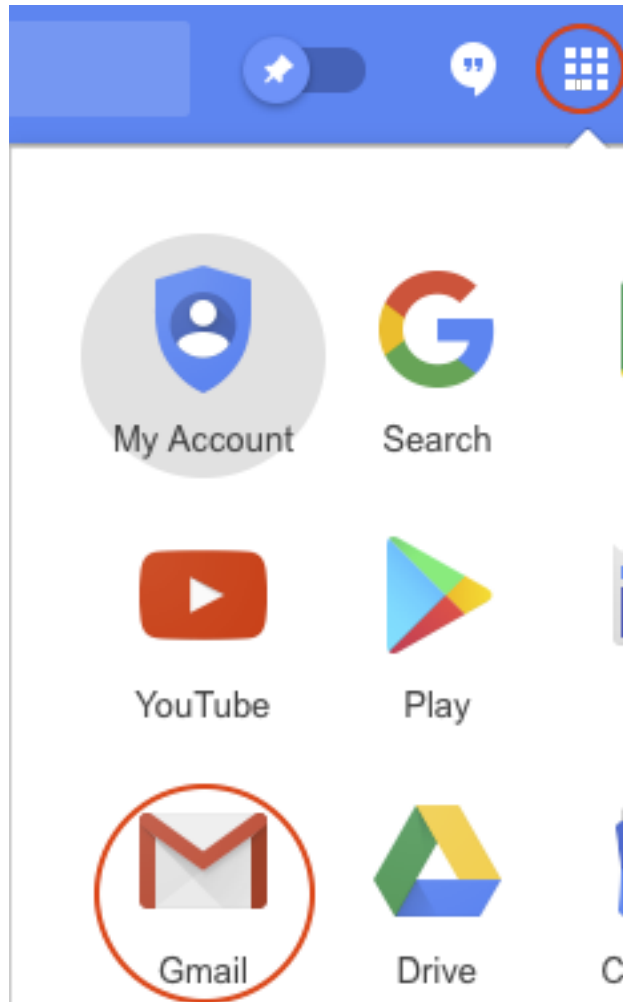
[Show advanced preferences](#)

4. Make sure that **Move** and **Permanently delete** are unchecked.
5. Make sure that **Mark spam as read** is unchecked.
6. You can optionally click **Show advanced preferences**, go to the **Backscatter** section, and select **With bounce spam: Do nothing** to have Fastmail ignore messages where it thinks a spammer impersonated you to send spam.

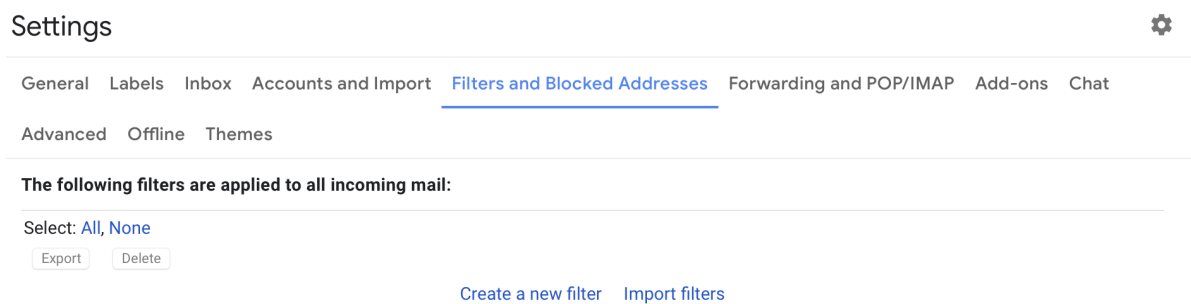
### 7.6.3 Turning Off the Gmail Spam Filter

SpamSieve users often find that Gmail's spam filter is unnecessary because SpamSieve catches more of the spam, and they want to turn off the Gmail filter to prevent any good messages from accidentally being caught. To disable Gmail's junk mail filter:

1. If you normally log into <https://gmail.com> in your browser, do that now and then move on to Step 2. If you normally use <https://inbox.google.com>, you can get to regular Gmail by clicking the 3×3 grid button at the top and then clicking the Gmail icon:



2. Click the gear at the top right, choose **Settings**, then click on **Filters and Blocked Addresses**.



3. Click **Create a new filter**. Enter `{(to:me) (deliveredto:USERNAME@gmail.com)}` in the **Has the words** field (replacing USERNAME with your actual Gmail username). Click **Create filter**.

From

To

Subject

Has the words {{(to:me) (deliveredto:USERNAME@gmail.com)}}

Doesn't have

Size

☐ Has attachment ☐ Don't include chats

Create filter

4. Make sure that **Never send it to Spam** is checked and click **Create filter**.

← When a message arrives that matches this search:

☐ Skip the Inbox (Archive it)

☐ Mark as read

☐ Star it

☐ Apply the label:

☐ Forward it [add forwarding address](#)

☐ Delete it

☒ **Never send it to Spam**

☐ Always mark it as important

☐ Never mark it as important

☐ Categorize as:

☐ Also apply filter to matching conversations.

Note: filter will not be applied to old conversations in Spam or Trash

6. Your filter should now look like this:

---

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | <b>Matches: {(to:me) (deliveredto:USERNAME@gmail.com)}</b> |
|                          | <b>Do this: Never send it to Spam</b>                      |

---

#### 7.6.4 Turning Off the GoDaddy Spam Filter

GoDaddy has two levels of junk mail filtering. The mail servers (both Exchange and IMAP) have built-in global spam filtering (affecting all users) that cannot be disabled. There are also per-user [additional settings](#) that can be disabled by selecting **Turn off filtering**.

#### 7.6.5 Turning Off the Hover Spam Filter

1. Log into your Hover Webmail at <https://mail.hover.com>.
2. Go to **Settings** ▸ **Spam Settings**.
3. Change the folder so that spam messages are moved to your inbox.

#### 7.6.6 Turning Off the iCloud Spam Filter

It is not possible to turn off iCloud's junk filter, and iCloud deletes some suspected spam messages without even putting them in your **Junk** mailbox. Thus, iCloud is not one of our [Recommended Mail Hosts](#).

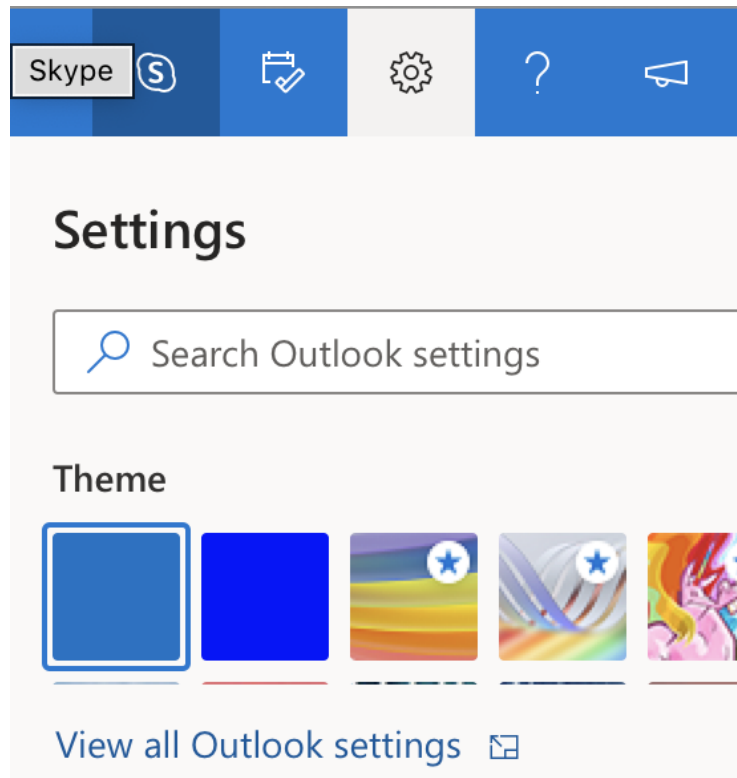
The [Consolidating Spam From Multiple Filters](#) section describes some ways to work around iCloud's spam filter.

#### 7.6.7 Turning Off Microsoft Spam Filters

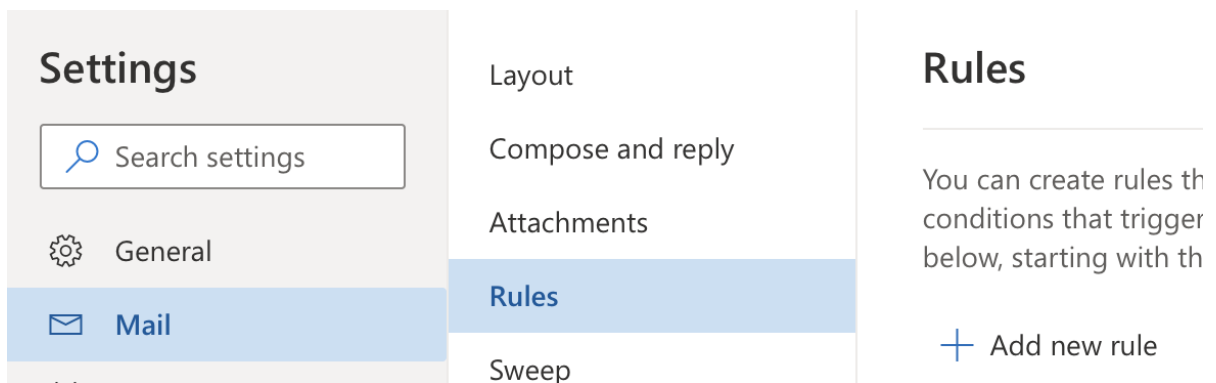
To turn off the server junk filter an for Outlook.com, Hotmail, or Office 365 mail account:

1. Log into the account using your Web browser, e.g at <https://outlook.live.com>.
2. Click on the gear icon at the top right, then click **View all Outlook settings**.





3. Click on **Mail**, then **Rules**, then **Add new rule**.



4. Set the rule's name to **Turn off Spam Filter**, set the condition to **Apply to all messages**, and set the action to **Move to Inbox**.

## Rules

Save

Discard



✓ Turn off Spam Filter

✓ Add a condition

Apply to all messages ▼

[Add another condition](#)

✓ Add an action

Move to ▼

Inbox ▼

[Add another action](#)

[Add an exception](#)

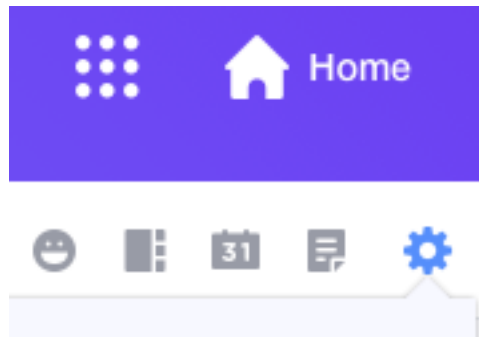
☒ Stop processing more rules ⓘ

5. Click the **Save** button.

### 7.6.8 Turning Off the Yahoo Mail Spam Filter

#### New Yahoo Mail

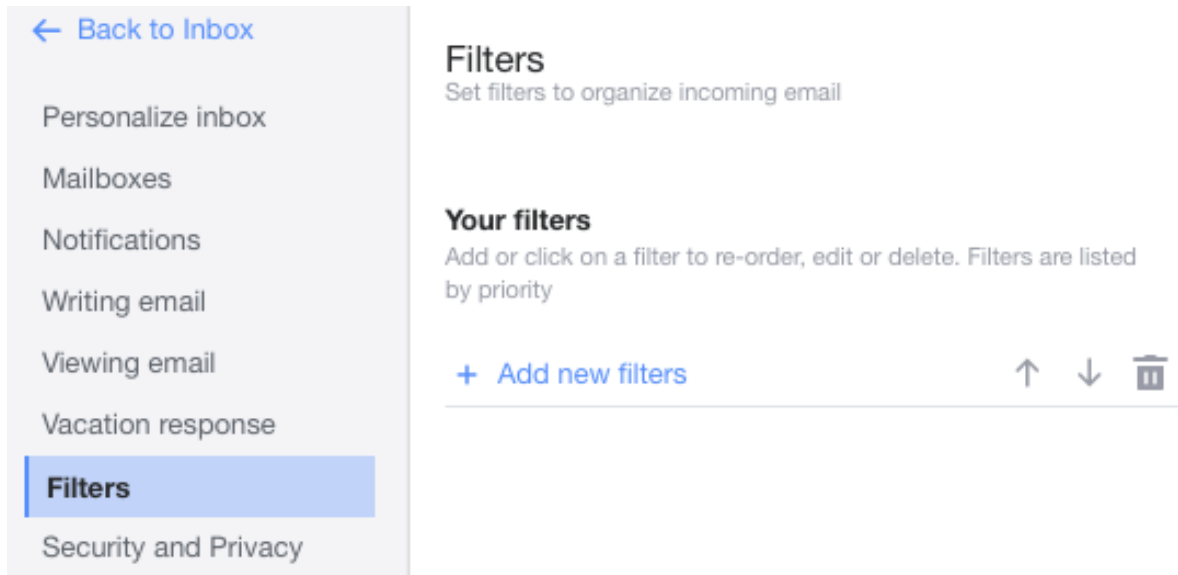
1. Log into your Yahoo Mail at <https://mail.yahoo.com>.
2. Click on the gear menu.



3. Click on **More Settings**.

... More Settings

4. Click on **Filters**.



5. Click + **Add new filters** and create a filter named **Turn Off Spam Filter**, with **From contains @** that moves the messages to **Inbox**.

## Edit Filter

### Filter name

Turn Off Spam Filter



Name your Filter

### Set rules

▼ From

contains



@



☐ Match case

› To/CC

› Subject

› Body

### Choose a folder to move to

Inbox



or

Folder name

Save

Cancel

6. Click **Save**.
7. Make sure that the new rule is at the bottom of the list. You can move it by selecting the rule and clicking the down-arrow button.

## Classic Yahoo Mail

1. Log into your Yahoo Mail at <https://mail.yahoo.com>.
2. Click on the gear menu.



3. Click on **Settings**, then **Filters**.

The screenshot shows the 'Settings' window for Yahoo Mail, specifically the 'Filters' section. On the left is a sidebar with navigation links: 'Viewing email', 'Writing email', 'Accounts', 'Vacation Response', 'Filters' (highlighted in blue), 'Security', and 'Banned Addresses'. Below these links, it shows '1TB of storage' and '0.01% used' with a note 'Space for 54 million more emails'. The main area is titled 'Sort incoming messages into folders' and contains a list of filters. At the top of this list are buttons for 'Add', 'Edit', and 'Remove', along with up and down arrow buttons. The first filter in the list is 'Turn Off Spam Filter', which is highlighted. Below the filter list, it says 'Deliver to "Inbox" if' followed by a bullet point: 'From contains "@"'. At the bottom of the window are 'Save' and 'Cancel' buttons.

4. Click **Add** and create a filter that matches @ in the sender and delivers the messages to **Inbox**.

Add a new filter
×

Filter Name

If an incoming message meets all of these conditions

|         |          |                                |                                     |
|---------|----------|--------------------------------|-------------------------------------|
| From    | contains | <input type="text" value="@"/> | <input type="checkbox"/> Match case |
| To/CC   | contains | <input type="text"/>           | <input type="checkbox"/> Match case |
| Subject | contains | <input type="text"/>           | <input type="checkbox"/> Match case |
| Body    | contains | <input type="text"/>           | <input type="checkbox"/> Match case |

Then move the message to this folder

- Click **Save**.
- Make sure that the new rule is at the bottom of the list. You can move it by selecting the rule and clicking the down-arrow button.

### 7.6.9 Turning Off Other Spam Filters

Many mail hosts offer [SpamAssassin](http://spamassassin.apache.org)<sup>99</sup> or a similar filter. Make sure the filter is set not to add **\*\*Junk\*\***, **[Spam]**, or another tag to the message's subject. Also, try to configure the filter not to move the messages out of the inbox. It is actually good if you can leave the filter on, but set so that it only tags the message's headers (e.g. by adding **X-Spam-Status** and **X-Spam-Report** headers). This will allow SpamSieve to incorporate the work that the server filter has done into its analysis.

## 7.7 Why does a message disappear or go back to the spam mailbox after I train it as good?

When you train a message in the spam mailbox as good, SpamSieve normally moves it back to the inbox. Mac Mail programs do not automatically re-apply rules (or SpamSieve) to old messages, so normally the message will stay in the inbox. However, there are several reasons that a message might stay in the Spam mailbox, "bounce back" to the Spam mailbox, or disappear from the Spam mailbox but not appear in the inbox:

- When you train a message as good, SpamSieve will purposely leave it in its current mailbox if:

<sup>99</sup><http://spamassassin.apache.org>

- You’ve used the **Change Settings** command to tell SpamSieve not to move trained messages to the inbox. Please see the [Change Settings \(Apple Mail\)](#) and [Change Settings \(Outlook\)](#) sections of the manual for more information.
  - SpamSieve thinks the message is not in a spam mailbox or the trash. SpamSieve knows common names of spam/junk mailboxes. You can each it a custom name using the **Change Settings** command.
2. When SpamSieve moves the message to the inbox, a server filter or a mail program on another computer may see the message as new and move it elsewhere. The other computer might think the message is spam and move it right back to the shared [server spam mailbox](#). Or, if the other computer is using a local spam mailbox, it would move the message *off* the server and into the spam mailbox *on that computer*. This would make it appear—on the first computer—as though the message had disappeared, but it would still be accessible in the local mailbox on the second computer.

For more information about multi-computer setups, please see the [SpamSieve and Multiple Macs](#) section. You can also use the [Change Settings \(Apple Mail\)](#) command to tell SpamSieve not to mark messages as unread when you train them as good. This may prevent other computers from seeing them as new messages.

3. If the message is moved to the inbox of an account that’s marked as inactive/disabled in Mail’s preferences, it will not be visible in Mail because that inbox is hidden. Normally, SpamSieve only moves messages to the inbox of an enabled account, however there is a bug in the macOS 10.15 Catalina version of Apple Mail that causes an error when SpamSieve asks if an account is enabled (FB7035263). Thus, if the disabled account is the [best match](#) for the message, SpamSieve could move it there. Versions 2.9.38 and later of the SpamSieve plug-in work around this Mail bug; you can choose [Install Apple Mail Plug-In](#) to make sure that you have the latest version of the plug-in installed.

You can enable the account in Mail’s preferences to view its inbox and find the “missing” messages.

4. The message might be in an inbox, just not in the one that you expected. Please see the [Why do good messages move to the wrong inbox when trained in Apple Mail?](#) section.
5. It’s possible that moving a message can make it disappear from Apple Mail due to a bug in macOS 10.15 and macOS 11 that affects a small percentage of users. You can avoid the bug by making sure that your inbox and Spam mailbox are stored in the same location, e.g. by [Using a Spam Mailbox on the Server](#). (If you have multiple mail accounts, you can use [Separate Spam Mailboxes for Each Account](#).) Please see the [Backing Up Messages](#) section of the manual for additional information.
6. It’s possible that moving a message can make it disappear from Apple Mail if Mail’s database is damaged. The message file is usually still visible on your Mac and on the server. To make the message re-appear in Mail, please see the [How can I rebuild Apple Mail’s database?](#) section.
7. Messages can “bounce back” to the spam mailbox due to being refiltered by another computer (#2), having a disabled account (#3), a server error, or a damaged Mail database (#5).

If you want to be extra careful to prevent any potential problems when moving messages, you can:

1. Use the **Change Settings** command to tell SpamSieve not to ask Mail to move messages when training.

2. Option-drag a message to another mailbox to make a backup copy of it.
3. Set SpamSieve to [automatically back up](#) all the messages that it sees, so that if Mail loses a message you'll still have a copy.

## 7.8 Does SpamSieve protect me from viruses?

Computer viruses generally do not cause problems for Mac users because there is no automated way for them to execute their malicious code. If you receive a virus in an e-mail attachment, it will not do anything if the message is just sitting in your inbox. Even opening the attached file is not, by itself, dangerous because macOS will not execute code from a single file. You would need to, for example, decompress the ZIP archive and then double-click the extracted `.app` file. Even if you do all this, the Mac is likely to warn you that you are launching an unknown application.

SpamSieve will generally classify messages with viruses as spam and move them to the **Spam** mailbox. This will prevent them from cluttering your inbox and provide some protection if you access your mail on a Windows PC (where attached `.exe` files can more easily cause harm).

### Anti-virus Software

If you are running anti-virus software, it is normal for it to find viruses in your **Spam** mailbox and in SpamSieve's **False Negatives** folder (if you've enabled the [Save false negatives to disk](#) preference). You can safely ignore these warnings because the viruses are embedded in the e-mail messages and are inert. It's also safe to delete the false negative files; they are only used when troubleshooting SpamSieve.

Anti-virus software such as Avira and Bitdefender can interfere with the operation of Apple Mail. One manifestation is that the software will find messages with viruses, which SpamSieve has put in the **Spam** mailbox, and delete the message files or move them to a holding area. Mail will then report errors because the files are no longer where it was expecting to find them, and this may prevent you from deleting the messages in Mail. You can get rid of the orphaned messages in Mail by [rebuilding its database](#). However, it is better to configure your anti-virus software so that it doesn't touch Mail's files. For example, in Avira, go to the **Real-Time Protection** settings, then **Basic Settings**, and change the **Default action if a thread is found** so that files are *not* moved into quarantine.

## 7.9 Does SpamSieve stop Web bugs?

A [Web bug](#)<sup>100</sup> is a tracking image in an HTML-formatted e-mail message. The image is referenced on a remote server, rather than included as an attachment to the message. When a mail client displays the message, it loads the image from the remote server. When the server receives the request for the image data, it knows that the e-mail has been read, and it can record the address of the computer that requested the image. Additionally, the image's URL may include tracking information such as your e-mail address, so the server can tell who read the e-mail.

Some legitimate mailing list providers use Web bugs to track how many of their messages were read, when they were read, and where (approximately) the recipients are located.

Spammers use Web bugs to track who is reading their messages. This lets them tell which e-mail addresses

---

<sup>100</sup>[http://en.wikipedia.org/wiki/Web\\_bug](http://en.wikipedia.org/wiki/Web_bug)



are valid as well as which variants of their message content get through spam filters. An e-mail address that is known to be valid is likely to receive more spam.

SpamSieve protects you against Web bugs by telling the mail program not to load remote images for messages that it thinks are spam. Since SpamSieve catches almost all spam messages, you only risk triggering a Web bug if SpamSieve lets a spam message through *and* you view that message. (If you know that a message is spam and don't want to select it to train it as spam, you can use the [drone setup](#) and drag the message to the **TrainSpam** mailbox.)

*Note:* SpamSieve does not tell Apple Mail on macOS 10.15 not to load remote images because this triggers a Mail bug that can prevent rules from moving messages to the proper mailbox.

For full protection, most mail clients have an option to disable the automatic loading of remote images for *all* messages, rather than just known spams. The downside to this approach is that to fully view a good message containing remote images you would need to click an extra button to tell the mail client to load the images.

Since SpamSieve is highly accurate, most users opt for the convenience of its automatic protection. If you want full protection and don't mind manually loading the images for all your messages, follow the these instructions for your mail client:

### Apple Mail

In the **Preference** window, click on the **Viewing** tab. Make sure that **Load remote content in messages** (called **Display remote images in HTML messages** prior to macOS 10.14) is unchecked.

### Airmail

In the **Preferences** window, click on the **General** tab. Make sure that **Autoload Remote Images** is unchecked.

### GyazMail

In the **Preferences** window, click on the **Display** tab. Make sure that **Show remote images in HTML messages** is unchecked.

### MailMate

In the **Preferences** window, click on the **Security** tab. Make sure that **Image Blocking** is checked and set to **All Messages**.

### Mailsmith

Mailsmith does not display remote images, so no setting is necessary.

### Outlook

In the **Preferences** window, click on **Reading**. Make sure that **Automatically download pictures from the Internet** is set to **Never**.

### Postbox

In the **Preferences** window, click on the **Privacy** tab. Make sure that **Block loading of remote images in mail messages** is checked.

### PowerMail

In the **Preferences** window, click on **HTML reader**. Make sure that **Download external pictures if connected, for non spam messages** is unchecked.

You can use [Email Privacy Tester](#) to verify that remote content is not being loaded.

## 7.10 Does SpamSieve bounce spam messages back to the sender?

SpamSieve does not have a feature to “bounce” spam messages back to the sender, e.g. by sending an e-mail reply saying that the message was not delivered. Apple Mail used to have a built-in **Message ▸ Bounce** command, but Apple has removed it.

The thought behind bouncing is that a spammer will stop sending to your address if he thinks that the address was invalid and his message didn’t get through. Unfortunately, sending a “bounce message” back would be ineffective or even counter productive for a variety of reasons:

1. *Spammers probably don’t care.* They have lists of thousands or millions of e-mail addresses, and it’s cheap to keep sending messages to the entire list. They may get paid based on the size of their list, no matter whether all the addresses are valid. In any case, it wouldn’t be worth the effort to prune it down.
2. *You can’t contact them.* Even if you believe that spammers care, your bounce message probably wouldn’t get to them. Spammers use hijacked machines and forged return addresses, so if you reply to a spam message you’re likely sending your bounce to an invalid address or to an innocent bystander.
3. *If you could, it might be bad for you.* There is a narrow window of time in which rejecting a spam message might work. When the mail server is in the process of receiving a message, it’s talking to the sending server, and so theoretically it could communicate that the address is invalid. By the time the message has been delivered to your account, downloaded by the mail program on your Mac, and filtered by SpamSieve, this window has long since closed. At this point, if the spammer were listening, he’d already know that the message had been delivered. If you were able to get a bounce back to him, he’d know that it was a fake bounce. The original message must have gotten all through, so he should send you *more* spam.

Since bouncing doesn’t work, it would be a waste of your time and network resources to do it. Including such a feature in SpamSieve would falsely imply that it should be used.

## 7.11 Does SpamSieve prevent me from receiving messages?

### Spam Messages

SpamSieve does not prevent spammers from sending you spam. This is not possible to do. However, since SpamSieve [protects you from viewing](#) the spam that you do receive, the spammers will not see their messages get through, so they are less likely to send you more.

SpamSieve also does not block spam messages from being received by your Mac. This would be dangerous because if it made a mistake (no filter can be perfect) you could completely miss a good message.

Instead, what SpamSieve does is make sure that incoming spam messages end up in your spam mailbox rather than your inbox. No messages are deleted without your knowledge, so you always have the opportunity to review them.

You can [optionally](#) configure SpamSieve so that messages from known spam senders go directly to the trash rather than to the spam mailbox.

## Good Messages

SpamSieve is designed with safety in mind so that, even if there is a bug in SpamSieve, it will never prevent you from receiving good messages or damage your local mail store. This follows directly from how SpamSieve works:

- SpamSieve does not communicate with your mail server at all. It does not need or affect your network connection or change whether your mail client is online or offline.
- Messages are not received *through* SpamSieve. It does not sit between your mail client and mail server. Instead, *after* your mail client has downloaded the new messages, it asks SpamSieve which of them are spam and moves those to the spam mailbox.
- SpamSieve does not read from or write to your mail client's data store. Instead, it simply decides whether a message is spam and lets the mail client itself move the message from the inbox to the spam mailbox. If SpamSieve thinks that a message is good, it doesn't touch it at all.
- SpamSieve does not affect how your mail program filters good messages. It moves the spam message to the spam mailbox, where they stay; the good messages are processed by your other rules as normal.
- SpamSieve does not touch or even see your sent messages. It only sees the messages that the mail client specifically sends to it for analysis: new, unread messages that arrive in the inbox and messages that you manually train it with.
- Some spam filters make changes to the messages that they process, e.g. adding subject or headers tags to indicate whether they are spam. SpamSieve does not modify the messages in any way, so there is no possibility of it damaging them.

## Troubleshooting

If you are missing e-mail messages or seem to not be receiving them, here are some things to check:

1. Because of the design described above, it is impossible for SpamSieve to cause you to lose messages or to interfere with the connection between your mail client and mail server. That said, people sometimes want to “know for sure” that SpamSieve is not the cause of the problem. You can see this by following the instructions in the [Uninstalling SpamSieve](#) section to temporarily disable SpamSieve or completely remove it.
2. Sometimes Mail loses track of messages when moving them from a server mailbox to a local mailbox. You can work around this by [Using a Spam Mailbox on the Server](#).
3. Use Web mail or a mail client on another computer or device to check the contents of your various mailboxes. If the messages show up there but not on your main Mac, you may need to [rebuild your local mail database](#).
4. Make sure that you have not created any rules on your mail server, on your mail client, or on another computer that delete messages or move them to the spam mailbox or trash. For example, a rule on one Mac that moves a message to a local mailbox will make it disappear from other computers that access the same mail account.
5. Make sure that a [junk filter on your mail server](#) is not moving or deleting messages before you see them.

6. Make sure that anti-virus software is not interfering. For example, if you are using Avast Mac Security, make sure that **Preferences** ▸ **Mail Shield Settings** ▸ **Scan secured connections** is unchecked. This can cause hangs when Apple Mail is receiving messages.
7. Try [disabling other Mail plug-ins](#) and see if that makes a difference.
8. [Check SpamSieve's log](#) to see whether there are **Predicted** entries for the missing messages. If so, this means that the messages went missing after they were downloaded to the inbox on your Mac. If not, this means that the messages never made it to your Mac.

## 7.12 SpamSieve Application Questions

### 7.12.1 Why doesn't my serial number work?

You need to enter the *serial 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 **Look Up My Serial Number** button.

### 7.12.2 Should I download SpamSieve from this free site?

No. We only recommend downloading SpamSieve from <https://c-command.com> and from reputable download sites such as Apple and MacUpdate. The [C-Command Store](#) lists all the vendors that are authorized to sell SpamSieve. Downloads from other sites may include adware or viruses.

The following sites:

DropDMG.downloads4mac.com  
DropDMG.install4mac.com  
DropDMG.macsoftware.com  
DropDMG.onFreeDownload.com  
EagleFiler.downloads4mac.com  
EagleFiler.install4mac.com  
EagleFiler.macsoftware.com  
EagleFiler.onFreeDownload.com  
SpamSieve.downloads4mac.com  
SpamSieve.install4mac.com  
SpamSieve.macsoftware.com  
SpamSieve.onFreeDownload.com

are *not* authorized to distribute our software. They have been a [source of confusion](#) because they often appear in ads at the top of search results for Bing, DuckDuckGo, and Yahoo. *We do not recommend downloading from these sites.* In many cases, they will say that they are offering an “official” copy of SpamSieve that is anything but. In fact, the installer asks for your administrator password, installs adware, and makes other changes that may damage your Mac.

CNET's Download.com offers a **Direct Download Link**, which is valid; however it also offers a more prominent **Download Now Installer Enabled** link, which we do not recommend. The CNET installer installs toolbar adware and changes browser settings. [This page](#)<sup>101</sup> explains how you can remove the toolbar.

<sup>101</sup>[https://web.archive.org/web/20151020025643/http://securemac.com/cnet\\_adware\\_removal\\_guide.php](https://web.archive.org/web/20151020025643/http://securemac.com/cnet_adware_removal_guide.php)

### 7.12.3 How can I hide SpamSieve's Dock icon?

To hide SpamSieve's icon from the Dock and the Command-Tab application switcher, click the special link below:

- To hide SpamSieve's Dock icon, [click this link](#)<sup>102</sup>.
- To show SpamSieve's Dock icon, [click this link](#)<sup>103</sup>.

SpamSieve will automatically remember these settings when you update to a new version.

A future version of SpamSieve will include a preferences checkbox for more easily hiding and showing SpamSieve's Dock icon, as well as a way to access this preference while SpamSieve's Dock icon and menu bar are hidden.

### If the SpamSieve Icon Is Still In Your Dock

macOS 10.14 and later include a section of the Dock for recent applications, and this can include the icons even of applications that have hidden their icons. To hide SpamSieve from this section, first quit SpamSieve. Then you can either:

- Click and hold on the SpamSieve Dock icon and choose **Options** ▸ **Remove from Dock** from the menu; or
- Drag the SpamSieve icon off the Dock; or
- Go to **System Preferences** ▸ **Dock** and uncheck **Show recent applications in Dock** to hide that section entirely.

### Opening Windows From Apple Mail

When SpamSieve's Dock icon is hidden, its menu bar is inaccessible. Therefore, 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 the [Open Window script](#) in order to do that.

### 7.12.4 How can I copy my training data to another machine?

#### SpamSieve's Data Files

SpamSieve stores its training data in the folder:

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

and it stores its preferences in the file:

---

<sup>102</sup>`x-spamsieve://default?k=HideDockIcon&v=YES`

<sup>103</sup>`x-spamsieve://default?k=HideDockIcon&v=NO`

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

You should back up both of these. (See the [How can I open the Library folder?](#) section for how to access them.)

### Moving or Copying SpamSieve to Another Mac (or User Account)

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.

Your SpamSieve [license](#) will be transferred when you copy the preferences file. You can also transfer it manually, by [looking up your order information](#).

When copying your SpamSieve setup to a Mac that didn't previously have SpamSieve installed, you'll need to put the SpamSieve application file in the **Applications** folder and do the [setup](#) in your mail program, but you can skip the initial training process because of the files that you copied above.

If you are copying the training data because you want to use SpamSieve on both Macs (rather than just moving it from one to the other), please see the [SpamSieve and Multiple Macs](#) section.

### Restoring From a Backup

1. Restore the SpamSieve folder and the `com.c-command.SpamSieve.plist` file that are mentioned above.
2. Go to the [SpamSieve Web site](#) and click the **Download** button.
3. Complete the installation steps in the [Installing SpamSieve](#) and [Using SpamSieve](#) sections, except that you can skip the initial training.

#### 7.12.5 Does SpamSieve launch automatically?

Yes. Once it's installed, you do not need to launch SpamSieve yourself. The mail client will automatically launch it as needed:

- Apple Mail will launch SpamSieve when it launches.
- The other mail clients will launch SpamSieve when they receive new e-mail messages that need to be processed or when you train a message as spam or as good. (For Outlook 365, you need to launch the **Outlook - Filter Mailboxes** app yourself; it will launch SpamSieve.)

If SpamSieve is not auto-launching as it should, please:

- Make sure that it's installed in the **/Applications** folder as described in the [Installing SpamSieve](#) section.
- Find the [appropriate section](#) to check the setup in your mail client.
- See the [Sending in an Error Report](#) section.

Although the SpamSieve application must be running in order to filter your mail, it ordinarily runs in the background with no user interface visible. The Dock icon can be [hidden](#) if desired, and you can also [set it](#) to quit when your mail client quits.

#### 7.12.6 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. Whether you're using multiple mail programs or just switching from one to another, you just need to follow the [setup instructions](#) once for each mail program. SpamSieve will automatically share its training data, rules, and statistics among all the mail programs.

#### 7.12.7 Why does SpamSieve need to access my contacts?

SpamSieve tries to read your macOS address book in order to prevent marking messages as spam if they were sent by one of your known contacts. This is controlled by the [Use macOS Contacts](#) preference.

It also reads which e-mail addresses are yours, in order to detect spam messages that may have been forged to come from your own address. This is controlled by the [Exclude my addresses](#) preference.

Normally, macOS will remember when you've given SpamSieve permission to access the contacts. If it keeps prompting you each time SpamSieve is launched, this is probably because you have modified your copy of the SpamSieve application, breaking its code signature. It is no longer necessary to modify SpamSieve to hide its Dock icon; please see the [How can I hide SpamSieve's Dock icon?](#) section.

#### 7.12.8 How can I open the Library folder?

The user library folder is stored at the path `/Users/<username>/Library/`. The way to access it is different depending on which version of macOS you are using:

##### macOS 10.12.3 and Later

The **Library** folder is hidden by default. To open it, click on Finder in the Dock. Click on the **Go** menu at the top of the screen, hold down the Option and Shift keys, and then choose **Library**. (Only one of Option and Shift is needed, but due to an [OS bug](#)<sup>104</sup>, which one you need to hold down can vary. Thus, it is easier to hold down both.)

Another way to access the **Library** folder is to choose **Home** from the **Go** menu, then type Command-Shift-Period to show invisible files, and then open the **Library** folder.

##### Mac OS X 10.7 Through 10.12.2

The **Library** folder is hidden by default. To open it, click on Finder in the Dock. Click on the **Go** menu at the top of the screen, hold down the Option key, and then choose **Library**.

Another option is to go to your home folder, choose **View** ▸ **Show View Options** and then make sure that **Show Library Folder** is checked.

---

<sup>104</sup><http://robservatory.com/more-about-macos-sierra-and-library-shortcut-keys/>

## Mac OS X 10.6

Click on Finder in the Dock, click on the **Go** menu, and choose **Home**. This will show your home folder, and you can open the **Library** folder directly.

### 7.12.9 What can I do if the corpus file is damaged?

A damaged corpus file can cause SpamSieve to crash at launch. Corpus file damage can be caused by crashes or disk errors.

There are several ways that you can fix this. First, quit both your mail program and SpamSieve. Then:

- If you have a backup from before the damage occurred, you can replace the file:

```
/Users/<username>/Library/Application Support/SpamSieve/Corpus.corpus
```

with a working copy. See the [How can I open the Library folder?](#) section for how to find this file and [this page](#)<sup>105</sup> for how to restore files via Time Machine.

- You can have SpamSieve reset the corpus for you:

1. Open your **Applications** folder and select SpamSieve.
2. While holding down the Command and Option keys on the keyboard, double-click the SpamSieve icon.

*Note:* If holding down the Command and Option keys does not work for you, you can instead enter this command:

```
defaults write com.c-command.SpamSieve ShowResetAlert YES
```

into Terminal and press Return before launching SpamSieve.

3. Click the **Reset Corpus** button in the window that pops up.
4. Re-train SpamSieve as described in the [Do an Initial Training](#) section.

- You can reset the corpus by deleting the file manually:

1. Open your **Library** folder. See the [How can I open the Library folder?](#) section for how to do this.
2. Find the file:

```
/Users/<username>/Library/Application Support/SpamSieve/Corpus.corpus
```

Inside **Library**, find the **Application Support** folder. Inside that is the **SpamSieve** folder. Inside that is the **Corpus.corpus** file.

3. Drag the **Corpus.corpus** file to the trash.
4. Re-train SpamSieve as described in the [Do an Initial Training](#) section.

---

<sup>105</sup><http://apple.stackexchange.com/questions/62402/how-to-restore-hidden-library-folder-in-time-machine>



### 7.12.10 What can I do if the statistics database is damaged?

A damaged statistics database can cause SpamSieve to crash, report internal errors, or show incorrect accuracy numbers in the [Statistics](#) window. Database damage can be caused by crashes or disk errors.

If you have a backup from before the damage occurred, you can quit SpamSieve and your mail program and replace the file:

```
/Users/<username>/Library/Application Support/SpamSieve/History.db
```

with a working copy. See the [How can I open the Library folder?](#) section for how to find this file.

Otherwise, you can have SpamSieve reset the database and start a new one. (This will not affect SpamSieve's training data or filtering accuracy.)

1. Quit SpamSieve and your mail program.
2. Open your **Applications** folder and select SpamSieve.
3. While holding down the Command and Option keys on the keyboard, double-click the SpamSieve icon.

*Note:* If holding down the Command and Option keys does not work for you, you can instead enter this command:

```
defaults write com.c-command.SpamSieve ShowResetAlert YES
```

into Terminal and press Return before launching SpamSieve.

4. Click the **Reset History** button in the window that pops up.

## 7.13 Apple Mail–Specific Questions

### 7.13.1 Why does the “Junk” mailbox appear in Apple Mail?

#### The Junk Mailbox

The [Setting Up Apple Mail](#) instructions have you turn off Mail's built-in junk mail filter, so it will not put messages in the **Junk** mailbox. However, it is normal for Mail to still *show* the **Junk** mailbox. (Older versions of macOS would always hide the **Junk** mailbox when Mail's filter was disabled.)

SpamSieve itself normally puts spam messages in the **Spam** mailbox, unless you've changed this as described in the [Changing the Name of the Spam Mailbox](#) section. You can tell which messages SpamSieve itself has processed by looking in [the log](#).

If your mail server has its own junk filter, it is normal for that filter to put spam messages in the **Junk** mailbox. Because the messages are filtered at the server level, they never arrive in your inbox. Your Mac therefore does not see them as new messages, so it does not apply your regular Mail rules (or the SpamSieve rule) to them. Since these messages are not SpamSieve [mistakes](#), you should not train them as spam.

The [How should I configure the junk filter on my mail server?](#) section has more information about server junk filters, how SpamSieve interacts with them, and how they can be turned off.

The [Consolidating Spam From Multiple Filters](#) section has more information about what to do if you don't want your spam to be split between two mailboxes, **Spam** and **Junk**.

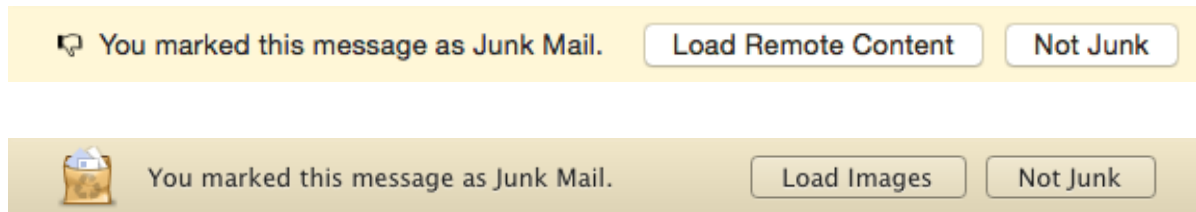
### iCloud's Junk Filter

As of April 2015, Apple has made its iCloud server junk filter much more aggressive. It is putting a lot more spam messages (and also some good ones) into the **Junk** mailbox. It also deletes some messages so that they do not appear in *any* mailbox. This affects all `icloud.com`, `mac.com`, and `me.com` e-mail accounts.

There is no way to [turn off iCloud's junk filter](#) and prevent it from putting messages in the **Junk** mailbox. There are, however, [various ways](#) to make SpamSieve put its spam into the same mailbox that iCloud's junk filter uses. SpamSieve can even re-filter the messages in the **Junk** mailbox to rescue good messages that iCloud put there. However, there is no way to rescue messages that were deleted without being saved into a mailbox. Since iCloud's junk filter cannot be disabled, your only choice is whether or not to use iCloud's mail service as a whole. If iCloud is not meeting your needs, we recommend switching to a [different mail provider](#).

### The Junk Bar and Messages Marked as Junk

It is normal for Mail to show a brown bar above some messages that SpamSieve or a server filter classified as spam. SpamSieve marks the messages as junk to [protect you from Web bugs](#). Do not click the **Not Junk** button. If the message is not spam, you should instead choose **SpamSieve - Train as Good** from the **Message** menu.



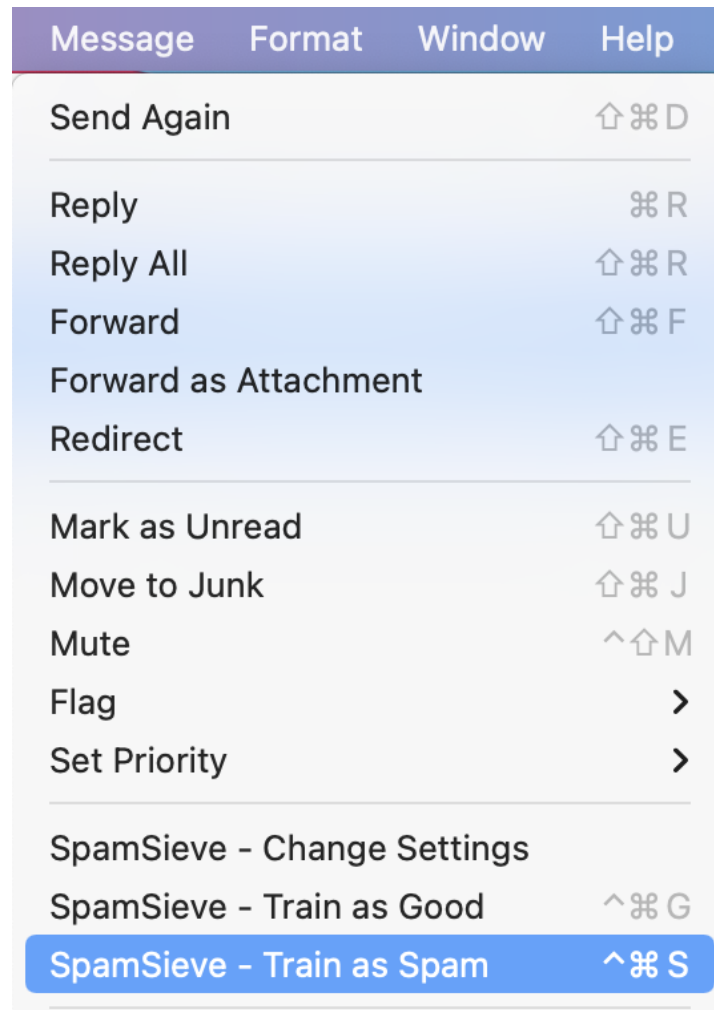
### Messages Moved to Invisible Junk Mailbox

In some cases—particularly prior to macOS 10.9—a server junk filter may move messages to a **Junk** mailbox that is hidden in Mail. This happens because Mail's own junk filter is off, so Mail hides the special **Junk** mailbox, not knowing that the server is using it. To fix this, you can tell Mail to use a different mailbox as the special **Junk** mailbox so that it hides *that* mailbox, and then makes the server's mailbox visible:

1. Choose **Mailbox** ▸ **New Mailbox...** to create a new mailbox inside your server account. Call the mailbox **HiddenJunk**.
2. Tell Mail to show it under the special **Junk** mailbox.
  - On macOS 10.12 and later, go to **Preferences** ▸ **Accounts** ▸ **Mailbox Behaviors** and choose **HiddenJunk** from the **Junk Mailbox** pop-up menu.
  - On macOS 10.11 and earlier, select the **HiddenJunk** mailbox and choose **Mailbox** ▸ **Use This Mailbox As** ▸ **Junk Mailbox**.

### 7.13.2 Why don't I see the SpamSieve commands in Apple Mail's Message menu?

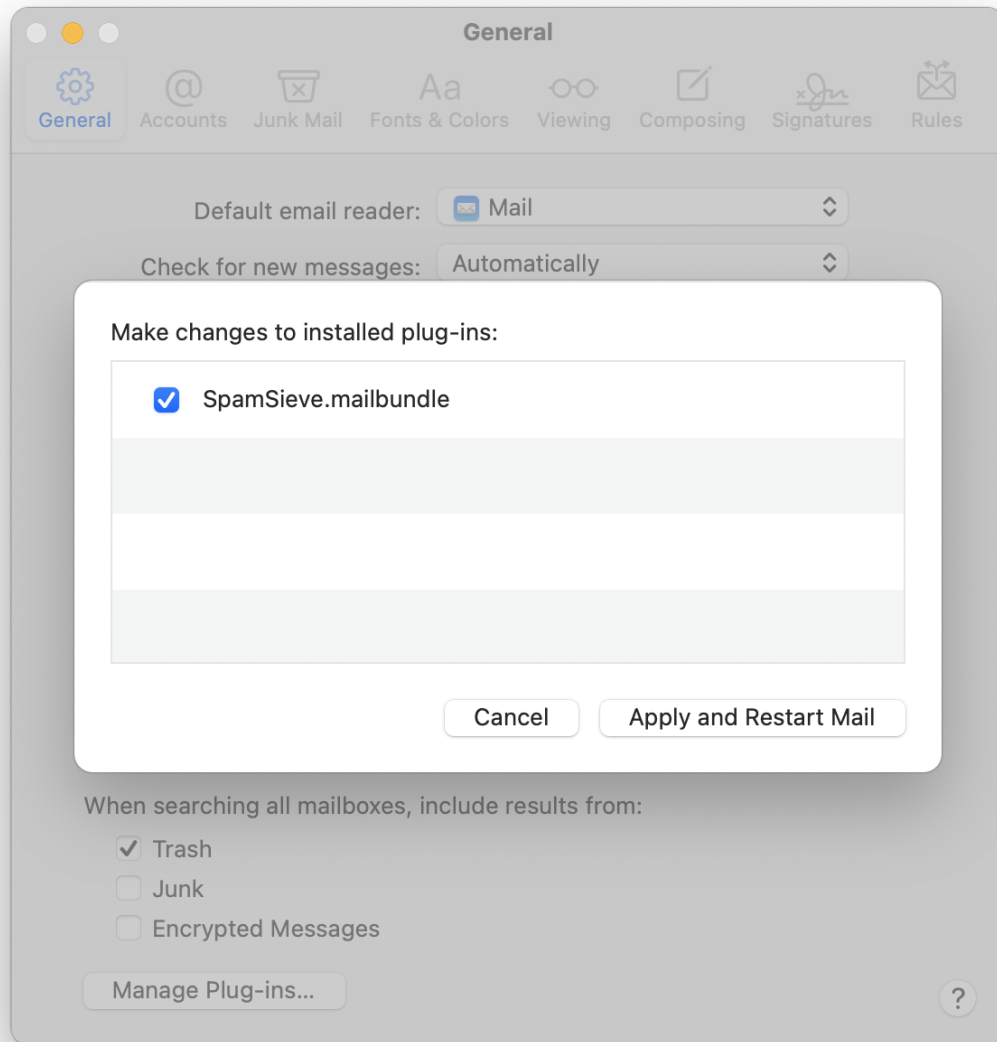
Normally, the **Message** menu in Apple Mail should contain several SpamSieve commands, after completing Step 2 of the [Setting Up Apple Mail](#) section.



If you don't see these commands, that means that SpamSieve's Mail plug-in is not loaded. If the plug-in is not loaded, you will not be able to train SpamSieve, and [Mail will move good messages to the spam mailbox](#) without consulting SpamSieve.

- The plug-in might have been disabled by an update to macOS. To prevent this from happening, it's best to update to the latest version of SpamSieve before updating macOS. See also the [Why does SpamSieve always need an update when macOS is updated?](#) section.
- To re-install the plug-in, choose [Install Apple Mail Plug-In](#) from the **SpamSieve** menu.

If you are using macOS 10.14 or later, you will need to click **Manage Plug-ins...** in Mail's preferences and enable **SpamSieve.mailbundle**. This is described in more detail in the [Enabling and Updating the Apple Mail Plug-In](#) section.



## Troubleshooting

First, see the troubleshooting information in the [Enabling and Updating the Apple Mail Plug-In](#) section if you don't see the plug-in in **Manage Plug-ins...** or if it doesn't stay enabled there.

If you still don't see the SpamSieve commands in the **Message** menu after relaunching Mail, try restarting your Mac. There may also be [errors reported in the Console](#) that point to the source of the problem.

In rare cases, Mail may be set not to load plug-ins and “stuck” so that this setting cannot be changed. To fix this, open the Terminal application and enter these commands:

```
cd ~/Library/Containers/com.apple.mail/Data/Library/Preferences/  
/usr/libexec/PlistBuddy com.apple.mail.plist -c 'Add EnableBundles bool YES'  
killall -SIGTERM cfprefsd
```

### 7.13.3 Why do good messages move to the wrong inbox when trained in Apple Mail?

When you train a message in the **Spam** or **Junk** mailbox as good, SpamSieve normally moves it back to your inbox. (You can adjust this behavior using the [Change Settings command](#).) If the messages are not going to the inbox, see the [Why does a message disappear or go back to the spam mailbox after I train it as good?](#) section.

If you have multiple mail accounts, you may sometimes find that SpamSieve moved the message to the inbox of a different account than the account that received the message.

The reason this happens is that Apple Mail does not keep track of which account received each message. Therefore, SpamSieve has to try to figure out the proper account by looking at the addresses in the message and the addresses associated with your accounts. Most of the time, this will work automatically. There are some exceptions, however:

- If you have multiple account aliases, SpamSieve will only know about them if they are configured in Mail's preferences. See "Adding Account Aliases" below.
- If you receive a "Bcc" message, where your address does not appear in the "To" or "Cc" header, SpamSieve can't tell which address it was sent to, so it can't determine the proper account. In that case, it will choose the first account in Mail that is not disabled.
- If you are using the `AppleMailTrainGoodGUIScripting` esoteric preference described in the [Faster Apple Mail Training](#) section, this bypasses SpamSieve's telling Mail which inbox to use. The message will always move to the inbox that you added to the favorites bar.

#### Adding Account Aliases

Some users configure multiple [aliases](#)<sup>106</sup> for a single e-mail account. For example, if your iCloud account is `john.q.public@icloud.com`, you may also want to receive messages sent to `johnp@icloud.com`.

Go to the **Accounts** tab of Mail's **Preferences** window and click on your account in the list. In this example, Mail's preferences would have the **User Name** entered as `john.q.public`. By default, the **Email Address** field would say `john.q.public@icloud.com`.

In order for SpamSieve to know which account's inbox to move a message to when you use the **Train as Good** command, you should enter all of your e-mail addresses (the main one and the aliases).

*macOS 10.12 and 10.13*

Click on the **Email Address** pop-up menu and choose **Edit Email Addresses**. Click the + button to add additional aliases.

*macOS 10.11*

---

<sup>106</sup><http://support.apple.com/kb/ph2622>

Click on the **Alias** pop-up menu and choose **Edit Aliases**. Click the + button to add additional aliases.

*macOS 10.10 and Earlier*

Enter the aliases into the **Email Address** field, separated by commas. In this example, the contents of the **Email Address** field should be:

`john.q.public@icloud.com, johnp@icloud.com`

For regular IMAP, Exchange, and POP accounts, you can edit the **Email Address** field directly. For iCloud accounts, first choose **Custom** from the **Alias** pop-up menu so that the **Email Address** field becomes editable.

### Per-Account Spam Mailboxes

Another way to help SpamSieve find the proper inbox is to have a separate spam mailbox for each account. If you are using the [standard setup](#), you have a single spam mailbox stored **On My Mac**. If you instead use per-account spam mailboxes, each spam message will be stored on the same account that received the message. SpamSieve can then move the message to the inbox on that same account, and the message will always end up in the right place.

To use this setup, follow the instructions in the [Using a Spam Mailbox on the Server](#) section and then follow the instructions in the [Separate Spam Mailboxes for Each Account](#) section, being sure to create each account's spam mailbox on that account.

#### 7.13.4 Why do I see spam messages in my “Unread” smart mailbox in Apple Mail?

A smart mailbox in Apple Mail is not a mailbox in the sense of “a place where messages are stored.” Rather, a smart mailbox is a “saved search” across multiple actual mailboxes. When you're viewing a smart mailbox, the message list shows the name of the mailbox that actually stores the message.

Thus, a smart mailbox that searches for unread messages will, by default, also find unread messages in the **Spam** mailbox. To avoid seeing spam messages in your Unread smart mailbox, make sure it's set up as follows:

- Contains messages that match *all* of the following conditions:
- Message is Unread
- Message is not in Mailbox **Spam**

#### 7.13.5 Why does the Spam mailbox in Apple Mail appear empty even though there's a number beside it?

Mail shows a number next to the **Spam** mailbox to indicate how many unread messages it contains. Sometimes you'll see the number, but when you click on the mailbox to see its contents you'll see either no messages or no unread messages. This may be because:

1. The unread messages are actually in a second mailbox, inside the **Spam** mailbox. If there's a triangle to the left of the mailbox icon, click to make it point down. This will reveal any mailboxes inside and allow you to access their contents.
2. Mail's database is damaged so that the numeric display is out of sync with the actual mail that's stored on your Mac and/or your server. You can fix this by [rebuilding Apple Mail's database](#).

#### 7.13.6 What can I do if my Spam mailbox in Apple Mail disappeared?

If you can't find your **Spam** mailbox, most likely it's still there but Mail is currently hiding it. To show the **Spam** mailbox:

1. From Mail's **View** menu, choose **Show Mailbox List** if necessary so that the mailboxes are visible.
2. Locate the **On My Mac** section of the mailbox list. It is typically below the **Mailboxes** and **Smart Mailboxes** sections of the mailbox list. You may need to scroll down in order to find this. (macOS may have made the scroll bars invisible, but you can scroll down by two-finger dragging on your Mac's trackpad or by using the scroll ball on the mouse.)
3. Move your mouse over **On My Mac** in the mailbox list. Then click the **Show** button that becomes visible at the right.



#### 7.13.7 Why are messages marked as spam in Apple Mail but not moved?

Sometimes SpamSieve may classify a message as spam, and [change its color](#) in Apple Mail, but the message does not move to the **Spam** mailbox; it remains in the inbox.

Here are some ways to fix this:

1. Make sure that your **SpamSieve** rule in Apple Mail looks like the one shown in Step 4 of the [Setting Up Apple Mail](#) section of the manual. If Mail loses track of the **Spam** mailbox, there may be no mailbox specified in the rule's actions, and so Mail will not move the spam messages.
2. You can test that the rule works and that Mail is able to move the messages by manually applying the **SpamSieve** rule. Select one of the messages in the inbox that was marked as spam and choose **Apply Rules** from the **Message** menu. You can check in the [Open Log](#) section of the manual whether SpamSieve predicted the message to be spam. If it did, but the message did not move, Mail may be encountering an error when it tries to move the message. Please see [Sending in an Error Report](#).
3. Sometimes Mail rules will not move messages that were processed immediately after the Mac woke from sleep. You can work around this problem by quitting Mail before sleeping your Mac or by changing the **Energy Saver** settings so that your Mac does not go to sleep automatically. You can also use the **QuitMailWhenMacSleeps** [esoteric preference](#) to make SpamSieve automatically quit Mail before the Mac sleeps and launch it when it wakes.

4. Recent versions of Mail have problems communicating with certain mail servers. Mail is more reliable at moving messages from the inbox to another mailbox on the same server than it is at moving the messages to a local mailbox. The [Using a Spam Mailbox on the Server](#) section of the manual explains how you can store your spam on the IMAP or Exchange server, so that Mail is better able to move it out of the inbox.
5. A bug in macOS 10.15 and macOS 11, affecting a small number of customers, can prevent messages caught by the normal **SpamSieve** rule from moving to the spam mailbox, leaving them colored in the inbox in Mail (though the server may show them as moved). It may help to [click this link](#)<sup>107</sup> to tell SpamSieve not to mark spam messages as junk on the server. You can also work around this by instead using an [Apple Mail Script Rule](#).
6. See whether the problem still occurs if you disable other Mail plug-ins, as described in the [Can other Apple Mail plug-ins cause problems with SpamSieve?](#) section.
7. Mail’s database may be damaged. Please see the [How can I rebuild Apple Mail’s database?](#) section of the manual.

#### 7.13.8 Why does SpamSieve always need an update when macOS is updated?

The top of the [SpamSieve Support](#) page always has the latest information about compatibility and public beta versions.

It is important (see below) to [update SpamSieve](#) before updating macOS. To prevent macOS from updating itself without asking you:

- macOS 10.14 and later: Go to the **Software Update** section of **System Preferences** and make sure that **Automatically keep my Mac up to date** is unchecked (or use the **Advanced...** button to tell it to only install security updates).
- macOS 10.13 and earlier: Go to the **App Store** section of **System Preferences** and make sure that **Install macOS updates** is unchecked.

#### Compatibility With macOS Updates

SpamSieve is developed using best practices, so it ordinarily continues to run normally when macOS is updated. That said, newer versions of SpamSieve are better at recognizing the latest types of spam—and contain many [other improvements](#)—so it’s best to run the latest version of SpamSieve [that your Mac supports](#). You can easily update to the latest version by choosing [Software Update...](#) from [the SpamSieve menu](#).

#### Compatibility With Apple Mail Updates

If you are using Apple Mail, you may have to update SpamSieve each time you update macOS. The reason for this is that SpamSieve uses a [plug-in](#) to integrate with Apple Mail. Each time Apple makes a change to Mail—which it does in most OS updates—there is a chance that the plug-in will stop working properly. Depending on the nature of the changes, an old plug-in running in a newer version of Mail could prevent Mail itself from working properly. (This has never actually happened with the SpamSieve plug-in, but we can’t rule out the possibility.)

---

<sup>107</sup>[x-spamsieve://default?k=AppleMailPlugInSetIsJunk&v=N0](https://x-spamsieve://default?k=AppleMailPlugInSetIsJunk&v=N0)



## Apple Mail Compatibility UUIDs

There are many [Mail plug-ins](#)<sup>108</sup>, and Apple understandably cannot test all of them, let alone their interactions with each other. Thus, starting around macOS 10.6, Apple adopted a policy where each plug-in declares (using UUIDs) which versions of Mail it has been tested with. If a plug-in has not been tested with the version of Mail that you're using, Mail will not load it.

The advantage to this system is that it makes Mail more reliable; it will not load any untested code. The disadvantage is that plug-ins like SpamSieve's, which make only a few hooks into very stable areas of Mail, usually do not require any changes to work with the new version of Mail. When Apple updates Mail, we have to ship a new version of the plug-in, with the new UUID to prove that it was tested with that version; customers have to update SpamSieve and its plug-in; but the new plug-in has the exact same code as the old one (aside from improvements unrelated to OS compatibility). Nevertheless, the UUID system does improve Mail's reliability and does not cause problems so long as customers are aware that they need to update SpamSieve (and any other plug-ins).

## Timing of SpamSieve Update Availability

Typically we ship an update to SpamSieve the same day that Apple updates macOS. Some customers have asked why SpamSieve updates do not become available until *after* Apple has shipped a macOS update.

From macOS 10.1 through 10.8, we would test SpamSieve with pre-release version of the OS. If a SpamSieve update was needed for compatibility with the new OS, we would try to ship the update before that version of the OS was released to the public. This was possible because there was generally only one set of UUIDs for each public release of macOS.

With later releases of macOS 10.8 through macOS 10.12 (but not 10.10.3 through 10.10.5), there are new UUIDs for most *pre-release* versions of macOS. With this new policy, we still test with pre-release versions of the OS, so we can have a SpamSieve update ready to go, but we cannot actually ship it until after the OS update ships. The reason for this is that the compatibility UUID that we need to declare is not known until we have the final shipping version of the OS update. This is the system working as designed: the UUID certifies that we have tested SpamSieve on the exact version of the OS that is running on your Mac.

## Update SpamSieve Before Updating macOS

The smoothest way to update macOS and SpamSieve is to update SpamSieve before updating macOS.

The reason for this is that if you update macOS first, and then open Mail, Mail will not load the old version of the SpamSieve plug-in. Without the plug-in loaded, you will not see the SpamSieve commands in Mail's **Message** menu, and Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve. If you get into this situation, quit Mail and then update SpamSieve. The next time you launch SpamSieve, it should detect that the plug-in was disabled by an OS update and reinstall the plug-in. If this does not happen automatically, you can choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#).

On the other hand, if you update SpamSieve before updating macOS, you will have the latest version of the plug-in when you launch the new version of Mail, so Mail will not disable it.

## Using Pre-Release Versions of macOS

If you are using a pre-release version of macOS, it will likely have a different compatibility UUID than the shipping version of SpamSieve. There are several ways to deal with this:

---

<sup>108</sup><http://www.tikouka.net/mailapp/>

- You can temporarily disable SpamSieve by unchecking its rule in Mail’s preferences. This will prevent [all your messages](#) from going to the **Spam** mailbox, but you will get spam messages in your inbox.
- You can use an [Apple Mail Script Rule](#) to filter your spam without needing to use an Apple Mail plug-in.
- There are public betas of SpamSieve corresponding to [public betas of macOS](#). You can click [this link](#)<sup>109</sup> (after installing SpamSieve) to sign up to receive beta versions of SpamSieve via the built-in [Software Update...](#) command. When updating to the beta, please read all of the release notes. You can click [this link](#)<sup>110</sup> if you want to stop receiving beta updates.
- If you are using a newer pre-release version of macOS that does not work with the public beta of SpamSieve, please try installing the Apple Mail plug-in and then use the **More Info** button in the error window to send us the error information [via e-mail](#)<sup>111</sup>.
- Previous versions of SpamSieve would let you hold down the Option key to install the Apple Mail plug-in on non-supported versions of macOS. This workaround stopped working with macOS 10.10 and has been removed.

### 7.13.9 Why do Apple Mail messages bounce back to the inbox after I train them as spam?

Sometimes when you train an uncaught spam message in the inbox as spam, the message will move to the spam mailbox and then appear to “bounce back” to the inbox. That is, the same message (not a new one that looks similar) will appear again in the inbox and no longer be in the spam mailbox. Usually, the same thing will happen if you move the message via drag and drop rather than training it with SpamSieve, which indicates that it’s a general problem with moving messages rather than something specific to spam filtering.

Typically, this means that Apple Mail and the mail server did not successfully move the message in the first place. Mail moved the message locally, but it did not get moved on the server, and so the next time Mail synchronized with the server it reinstated the message in the inbox.

Sometimes this is caused by a problem with Mail’s database, and you can fix it by doing a [complete rebuild of the database](#).

Other times, most commonly with Gmail, there can be a problem moving the message from the inbox (on the server) to a local mailbox (the **Spam** mailbox under **On My Mac**). If the mail server does not want to do this, it can help to instead set SpamSieve and Mail to use a [spam mailbox on the server](#), which lets the server instead move the message between two server mailboxes, which often works better.

### 7.13.10 How can I rebuild Apple Mail’s database?

Many common problems with Mail can be fixed by rebuilding all or part of its index database. For example:

- You have a mailbox that shows a number of unread messages in the mailbox list, but when you click on the mailbox there do not seem to be any unread messages inside.

<sup>109</sup>[x-spamsieve://default?k=MJTUpdateCheckerBetaKey&v=PublicBeta](#)

<sup>110</sup>[x-spamsieve://default?k=MJTUpdateCheckerBetaKey&delete=1](#)

<sup>111</sup>[mailto:spamsieve@c-command.com](#)

- Messages seem to have disappeared; they show up when you search your Mac using Spotlight but not when browsing or searching in Mail.
- A smart mailbox doesn't seem to be finding the messages that you think it should.
- You click on a mailbox that you know contains some messages, but Mail doesn't show any.
- Messages are colored as spam but remain in the inbox, even though your SpamSieve rule is set to move them to the **Spam** mailbox.
- You try to delete messages, but they come back or Mail reports an error.
- Mail is very slow at browsing or searching messages.

First, try a *quick rebuild*. Select the problem mailbox, go to the **Mailbox** menu, and choose **Rebuild**.

If this doesn't solve the problem, try a *complete rebuild*:

1. Quit Mail.
2. Locate the **Envelope Index** file. On macOS 11.0, the file is stored at:

```
/Users/<username>/Library/Mail/V8/MailData/Envelope Index
```

Open your user **Library** folder. (See the [How can I open the Library folder?](#) section if necessary.) Then open the **Mail** folder, then **V8**, then **MailData** to find the **Envelope Index** file.

- On macOS 10.15, the **MailData** folder is inside of the **V7** folder rather than **V8**.
  - On macOS 10.14, the **MailData** folder is inside of the **V6** folder rather than **V8**.
  - On macOS 10.13, the **MailData** folder is inside of the **V5** folder rather than **V8**.
  - On macOS 10.12, the **MailData** folder is inside of the **V4** folder rather than **V8**.
  - On macOS 10.11, the **MailData** folder is inside of the **V3** folder rather than **V8**.
  - On macOS 10.7 through 10.10, the **MailData** folder is inside of the **V2** folder rather than **V8**.
3. Once you've found the **Envelope Index** file, drag it to the trash. Also delete **Envelope Index-shm** and **Envelope Index-wal** (if they exist).

*Note:* Rebuilding the index database is normally perfectly safe. Even though it seems that you are deleting a file, Mail stores its primary copy of your message data elsewhere. When you delete the damaged database, Mail uses this primary copy to create a new index database. However, **please be careful if you are using macOS 10.15**. We've heard some [reports](#) that rebuilding the **Envelope Index** can lose messages in **On My Mac** mailboxes on macOS 10.15.0–10.15.2 due to a bug in Mail. If you are using macOS 10.15 prior to macOS 10.15.3, be sure that you have a backup first, and proceed with caution.

4. Relaunch Mail. It will welcome you as if you haven't used it before. This step may take a few minutes, as Mail searches through all of your stored messages to build your new database file. IMAP and Exchange messages will need to be re-downloaded from the server.

### 7.13.11 How can I reset Apple Mail's junk database?

A corrupt database for Mail's built-in junk mail filter can cause Mail to crash when processing incoming messages or when training messages with SpamSieve. To reset the database, find the LSMMMap2 file and drag it to the trash.

- On macOS 11.0, the file is stored at:

```
/Users/<username>/Library/Mail/V8/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V8, then MailData to find the LSMMMap2 file.

- On macOS 10.15, the file is stored at:

```
/Users/<username>/Library/Mail/V7/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V7, then MailData to find the LSMMMap2 file.

- On macOS 10.14, the file is stored at:

```
/Users/<username>/Library/Mail/V6/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V6, then MailData to find the LSMMMap2 file.

- On macOS 10.13, the file is stored at:

```
/Users/<username>/Library/Mail/V5/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V5, then MailData to find the LSMMMap2 file.

- On macOS 10.12, the file is stored at:

```
/Users/<username>/Library/Mail/V4/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V4, then MailData to find the LSMMMap2 file.

- On macOS 10.11, the file is stored at:

```
/Users/<username>/Library/Mail/V3/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V3, then MailData to find the LSMMMap2 file.

- On macOS 10.7 through 10.10, the file is stored at:

```
/Users/<username>/Library/Mail/V2/MailData/LSMMMap2
```

See the [How can I open the Library folder?](#) section. Open the Mail folder, then V2, then MailData to find the LSMMMap2 file.

### 7.13.12 Can other Apple Mail plug-ins cause problems with SpamSieve?

We try to ensure that SpamSieve is compatible with other [Apple Mail plug-ins](#)<sup>112</sup>. Nevertheless, it is possible for another plug-in—especially an old version—to prevent SpamSieve or Mail from working properly.

#### Known Issues

##### *GPGMail*

There is a known [bug](#) in the [GPGMail](#) plug-in that causes it to re-apply Mail’s rules (including SpamSieve) to non-new messages and even to sent messages.

##### *MailTags*

[MailTags](#) has generally been fully compatible with SpamSieve. Please make sure that you are using the latest version of MailTags. If you encounter any problems, see if disabling it helps.

#### Troubleshooting

If you are using multiple Mail plug-ins and seeing hangs, problems launching, or other unexpected behavior, it’s best to check whether the problem goes away when *only* the SpamSieve plug-in is installed.

- On macOS 10.14 and later, you can disable Mail plug-ins by unchecking them from **Preferences** ▸ **General** ▸ **Manage Plug-ins**...
- On earlier versions of macOS, Mail plug-ins can be installed in the global **Bundles** folder (which not all users will have):

`/Library/Mail/Bundles`

and also in the user **Bundles** folder:

`/Users/<username>/Library/Mail/Bundles`

To access this folder, see the [How can I open the Library folder?](#) section.

Please check both **Bundles** folders for any `.mailbundle` files/folders. You can temporarily disable a plug-in by dragging its `.mailbundle` to your desktop and then re-launching Mail.

If disabling the other Mail plug-ins fixes the problem:

- You have a temporary fix for the problem: uninstalling the other plug-ins.
- You can report the problem to us and to the other plug-in developer so that we can find a way for the plug-ins to work better together.

### 7.13.13 What can I do if Apple Mail is crashing?

Under normal circumstances, Apple Mail does not crash, whether or not you are using SpamSieve. If you find that Mail is crashing, here are some things that you can do:

---

<sup>112</sup><http://www.tikouka.net/mailapp/>

1. First, please [send us a crash report](#) so that we can look into the cause. Note that if you are seeing a spinning beachball cursor rather than a crash report window, Mail is probably *hanging* rather than *crashing*. In that case, you should instead [record a “sample” log](#) of Mail during the hang.
2. Often, it helps just to restart your Mac.
3. Make sure that any other Mail plug-ins are updated to their latest versions. If that doesn’t help, see whether [disabling](#) the other plug-ins stops the crashes.
4. The most common Mail crash that we see is due to a bug in Mail’s own junk mail filter. SpamSieve normally tells Mail which messages it thinks are junk in order to [protect you from Web bugs](#). [Resetting Mail’s junk database](#) may fix the problem.  
  
You can also tell SpamSieve not to mark the messages as junk if analyzing the spam messages is causing Mail’s filter to crash. To do this, click the link for `AppleMailPlugInSetIsJunk` in the [Esoteric Preferences](#).
5. In macOS 10.10, there is an Apple Mail bug that can cause crashes if you are using an Exchange account and have a rule that moves messages to a mailbox on the Exchange server. To work around this, make sure that you are using the [standard setup](#) with the **Spam** mailbox **On My Mac**.
6. In the **Accounts** preferences in **Mail**, for each account click on **Server Settings** (formerly **Advanced**) and make sure that **Automatically detect and maintain account settings** is unchecked. This option is not available for every type of mail account.
7. Try renaming the **SpamSieve** rule in Mail to **Move to Spam**. This will cause Mail to treat it like a regular rule, bypassing SpamSieve. If Mail still crashes when applying the rule, this will show that the crash is due to Mail moving the message to the spam mailbox and not because of SpamSieve.  
  
This test will cause Mail to move all incoming messages to the spam mailbox. After the test, you can disable the rule, move the messages back to the inbox, and use the **Message** ▸ **Apply Rules** command to re-filter them.
8. If Mail is crashing when applying the **SpamSieve** rule (regardless of the results of #4) you can try using an [Apple Mail Script Rule](#) instead of the regular **SpamSieve** rule. Because this uses a different code path in Mail, it may bypass the source of the crash.
9. SpamSieve works with a [variety of mail programs](#). You could temporarily use a different one, either for reading your mail or just for spam filtering. With an IMAP or Exchange mail account, you will see the same mailboxes and messages in each mail program.

## 8 Legacy Mail Programs

The following mail programs are discontinued, but they can still be used with SpamSieve.

### 8.1 Setting Up Airmail 1–3

These instructions apply to versions 1–3 of Airmail. For Airmail 4, please see the [Setting Up Airmail](#) section.

1. Make sure that you are using Airmail 1.3.1 (223) or later.
2. From the **Airmail 3** (or **Airmail 2**) menu, choose **Preferences...**
3. Click on the **Accounts** icon at the top of the window. For each IMAP account in the list:
  - a) Click on the **More** tab and look in the **Download** section.
  - b) Make sure **Message Content** is checked.
  - c) Make sure **Attachments** is checked.

POP accounts do not have the **Download** section, so you can skip this step for them.

Click the **Save** button.

4. Click on the **Advanced** icon at the top of the window and make sure that **Use SpamSieve** is checked.
5. Now it is time to train SpamSieve:
  - To train SpamSieve with spam messages, select the messages, Control-click, and choose **SpamSieve - Train as Spam** from the contextual menu. (Do not use the **Mark as Spam** command.)
  - To train SpamSieve with good messages, select the messages, Control-click, and choose **SpamSieve - Train as Good** from the contextual menu. (Do not use the **Mark as Not Spam** command.)

The [Do an Initial Training](#) section explains which messages (and how many of them) you should train.

On macOS 10.14 or later, the first time you try to train a message macOS will ask whether Airmail [can control](#) SpamSieve, and you should click **OK**.

SpamSieve will process new mail automatically. Messages that it thinks are spam will be moved to the **Junk** or **Spam** folder. Airmail will automatically launch SpamSieve when there are new messages that need to be filtered or when you train messages as spam or as good.

If you need to troubleshoot SpamSieve and Airmail, see the [Checking the Airmail Setup](#) section.

## Keyboard Shortcuts

If you prefer not to use the menu commands for training SpamSieve, you can set up keyboard shortcuts as follows:

1. Open **System Preferences**.
2. Click on the **Keyboard** icon.
3. Click on the **Shortcuts** (or **Keyboard Shortcuts** on older versions of macOS) tab.
4. Select **App Shortcuts** (or **Application Shortcuts** on older versions of macOS).
5. Click the **+** button.
6. For **Application**, select **Airmail 3** (or **Airmail 2** or **Airmail**).
7. For the **Menu Title**, enter **SpamSieve - Train as Spam**.

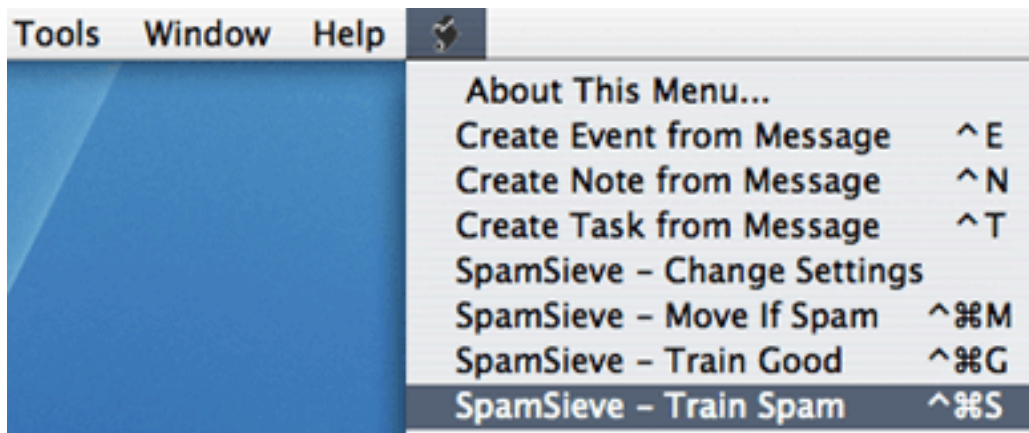
8. Click in the box next to **Keyboard Shortcut** and enter your desired shortcut. We recommend Command-Control-S.
9. Click the **Add** button.
10. Click the **+** button.
11. For **Application**, select **Airmail 3** (or **Airmail 2** or **Airmail**).
12. For the **Menu Title**, enter **SpamSieve - Train as Good**.
13. Click in the box next to **Keyboard Shortcut** and enter your desired shortcut. We recommend Command-Control-G.
14. Click the **Add** button.

When the keyboard shortcuts are set up correctly, you will see them in Airmail's **Message** ▸ **Mark as Reminder** menu.

## 8.2 Setting Up Entourage

This section applies to Entourage 2004 and 2008. Please see the [Setting Up Entourage v.X](#) section if you need to set up an older version of Entourage.

1. Go to Entourage's **Tools** menu and select **Junk E-mail Protection**. Turn off Entourage's junk filter by clicking **None** and then **OK**.
2. Switch to SpamSieve by clicking on its icon in the Dock. Go to the **SpamSieve** menu and choose **Preferences...** Make sure that [Use Entourage/Outlook address book](#) is checked and click the **Load** button, then the **Entourage** button.
3. Choose **Install Entourage Scripts** from the **SpamSieve** menu. After you quit and re-launch Entourage, you should see four SpamSieve items in Entourage's **Scripts** menu:

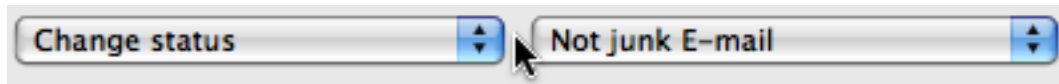


4. Choose **Rules** from Entourage's **Tools** menu. Click on the tab corresponding to the type of account you have (e.g. POP, IMAP, or Exchange). If you have more than one kind of account, you will need to repeat steps 4–6 for each account type.

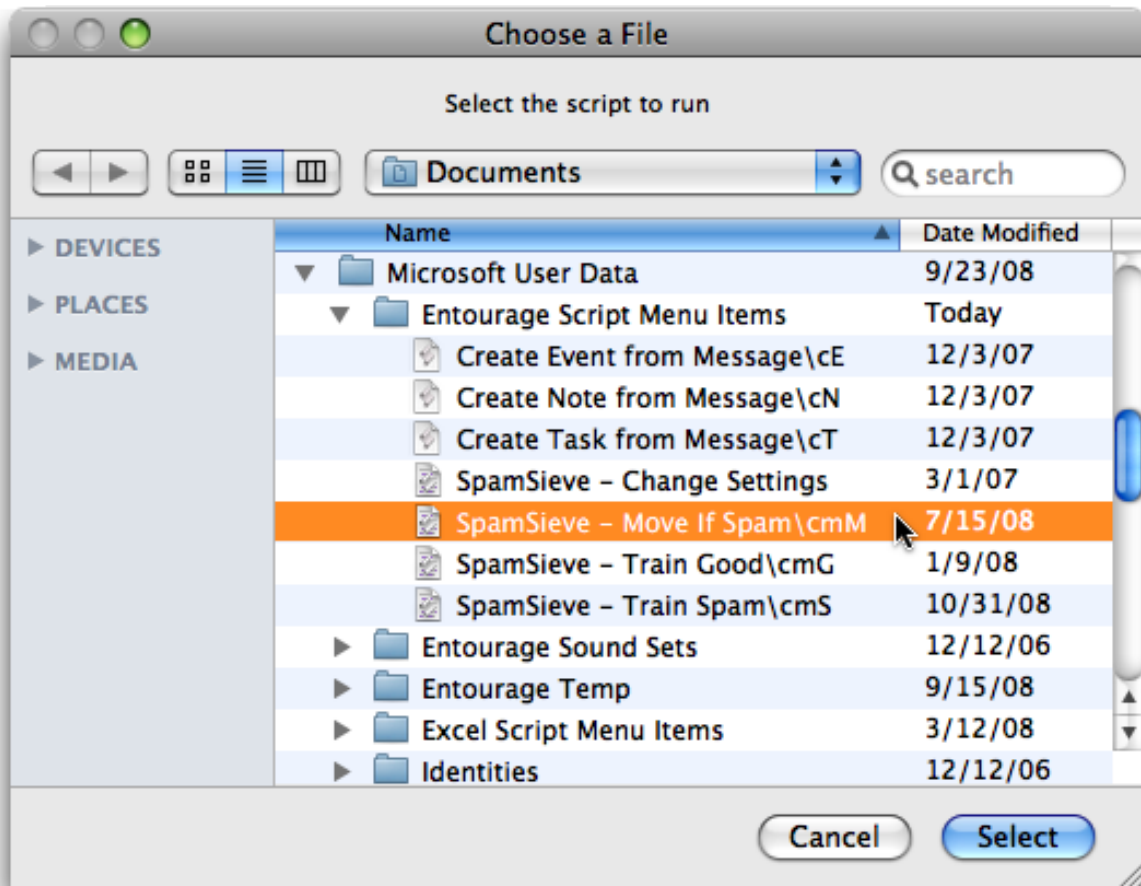


Click the **New** button. Change the name of the rule to **SpamSieve - Move If Spam**.

Click on the empty space between **Change status** and **Not junk E-mail**. Click **Remove Action** to delete the **Change status** action.



Click on the menu that says **Set category** and choose **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 (which is probably inside the **Microsoft User Data** folder inside your **Documents** folder):



Make sure that **Do not apply other rules...** is unchecked. The rule should now look like:



Click **OK** to close the **Edit Rule** dialog.

*Note:* 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.

*Note:* If you are using Gmail (via IMAP) or Exchange with Entourage, change the criterion from **All messages** to **Folder Is Inbox (<Account Name>)**.

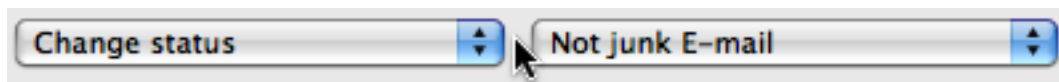
5. Click the **New** button to create a second rule. Change the name of the rule to **SpamSieve - Move Messages**.

Click on **All messages** and change it to say **Category Is Junk**.

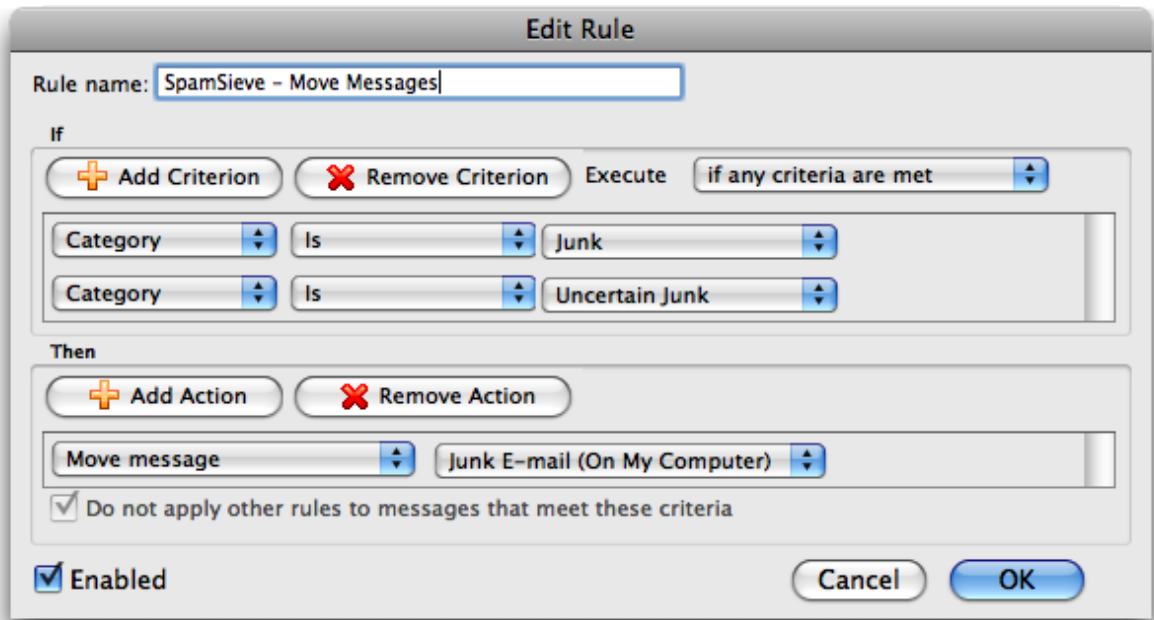
Click **Add Criterion**. Click on **From** for the new criterion and change it to say **Category Is Uncertain Junk**.

Click on **if all criteria are met** and change it to **if any criteria are met**.

Click on the empty space between **Change status** and **Not junk E-mail**. Click **Remove Action** to delete the **Change status** action.



Click on the menu that says **Set category** and choose **Move message**. Change the menu at the right from **Inbox** to **Junk E-mail**. The rule should now look like:



Click **OK** to close the **Edit Rule** dialog.

6. Make sure that the **SpamSieve - Move If Spam** rule appears at the top of the list in the **Rules** window. Directly below it should be the **SpamSieve - Move Messages** rule. You can change the order by dragging.
7. Now proceed to the [Do an Initial Training](#) section.
  - To train SpamSieve with spam messages, select one or more of them and then choose **SpamSieve - Train Spam** from Entourage's **Scripts** menu (as shown in the picture for Step 3, above).
  - 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:* The training commands will move locally stored messages to the **Junk E-mail** folder or the inbox. Due to limitations of Entourage, they do not move IMAP or Exchange messages. (Incoming spam messages *will* be automatically moved to the **Junk E-mail** folder.)

SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **Apply Rule** ▸ **All Rules** from the **Message** menu.

The above is all you need to know about using SpamSieve with Entourage. The [Entourage Customization](#) section explains some more advanced setup options.

### 8.2.1 Entourage Customization

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.

Additional customizations are described below:

## Change Settings

You can choose **SpamSieve - Change Settings** from Entourage's **Scripts** menu to customize SpamSieve's behavior in 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?

## Spam Message Categories

SpamSieve colors spam messages in Entourage using one of two categories:

### Junk

This is for messages that you mark as spam (using the **SpamSieve - Train Spam** command) and for most incoming messages that SpamSieve thinks are spam.

### Uncertain Junk

This is for incoming messages that SpamSieve thinks are spam, but whose scores are below the uncertainty threshold. For more information about scores and uncertainty, see the [A spam message is uncertain if](#) preference.

To change the colors associated with these categories, choose **Edit** ▸ **Categories** ▸ **Edit Categories**.

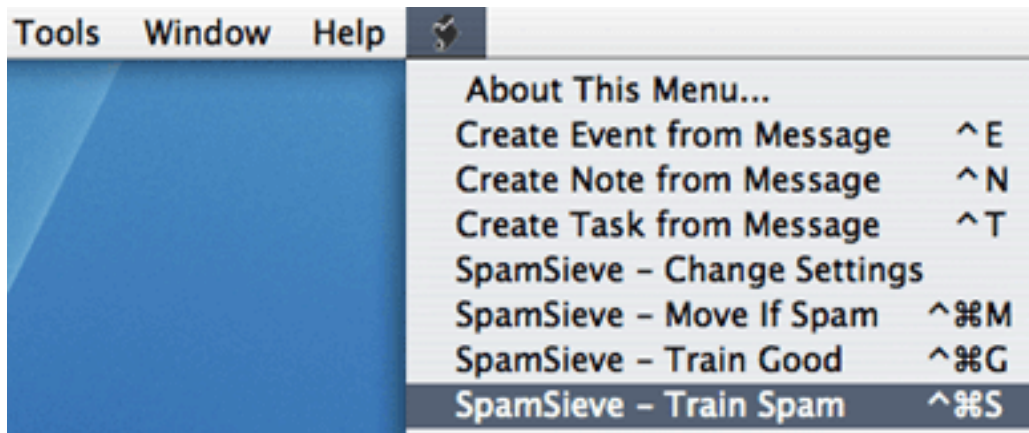
Normally, both **Junk** and **Uncertain Junk** messages are put into the same **Junk E-mail** folder. It is also possible to separate the messages by category. To do this:

1. Create a new folder in Entourage called **Uncertain Junk**.
2. Create a third rule called **SpamSieve - Move Uncertain Messages**. It should say “If Category Is Uncertain Junk, Then Move message Uncertain Junk.”
3. Drag the new rule between the **SpamSieve - Move If Spam** and **SpamSieve - Move Messages** rules.

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

### 8.3 Setting Up Entourage v.X

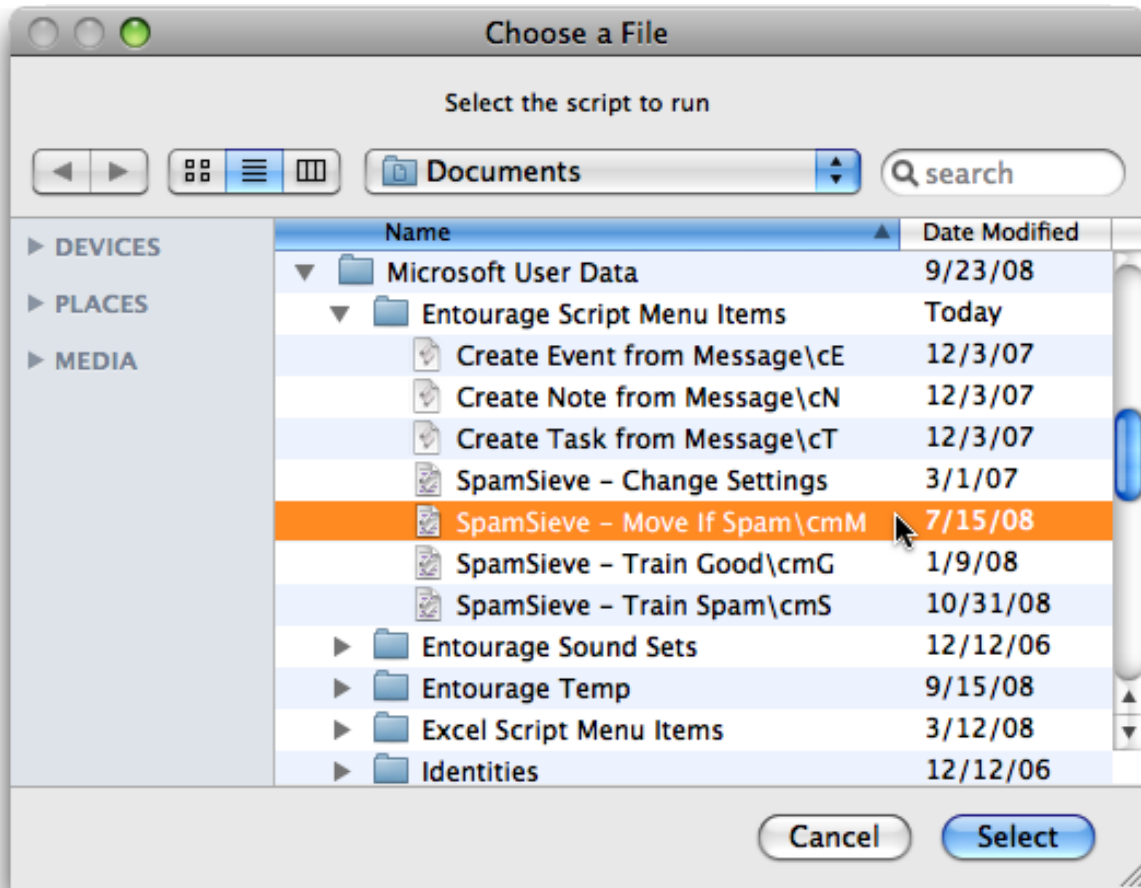
1. Go to Entourage’s **Tools** menu and choose **Junk Mail Filter**. Turn off Entourage’s junk filter unchecking **Enable Junk Mail Filter**.
2. Double-click the SpamSieve application and choose **Preferences** from the **SpamSieve** menu. Make sure that **Use Entourage/Outlook address book** is checked, 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).
3. Choose **Install Entourage Scripts** from the **SpamSieve** menu. Quit and re-launch Entourage; then you should see four SpamSieve items in Entourage’s **Scripts** menu:



4. 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 choose the first action. Click **Remove Action** to delete the **Change status** action. Click on the menu that says **Set category** and choose **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 (which is probably inside the Microsoft User Data folder inside your Documents folder):



*Note:* 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.

- Click **OK** and drag the SpamSieve rule to the top of the list.
- Now proceed to the [Do an Initial Training](#) section. 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.

SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **Apply Rule** > **All Rules** from the **Message** menu.

The above is all you need to know about using SpamSieve with Entourage. The [Entourage Customization](#) section explains some more advanced setup options.

## IMAP Accounts

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.

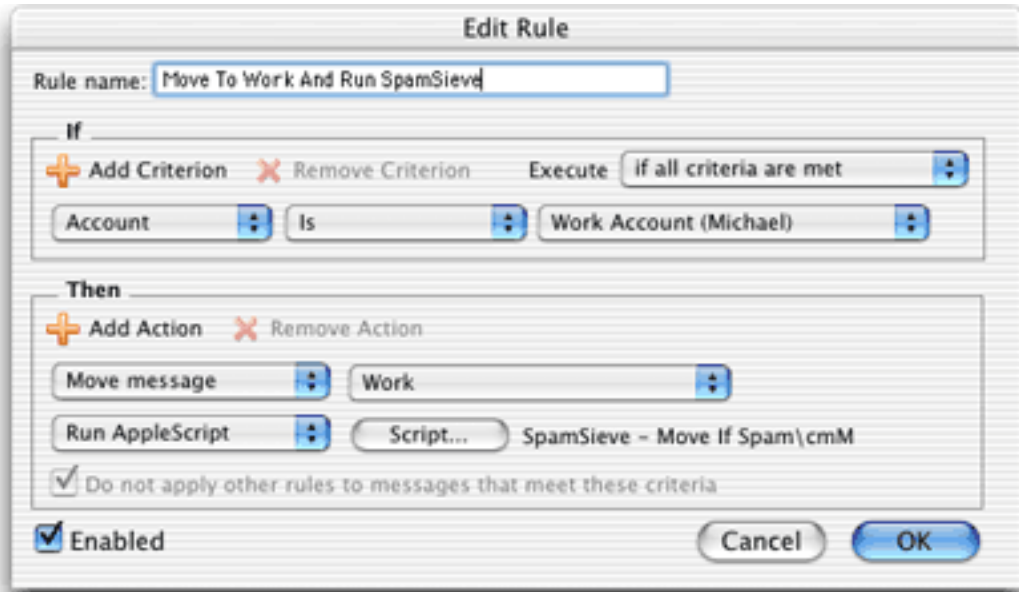
### Rule Tips

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.





## 8.4 Setting Up MailForge

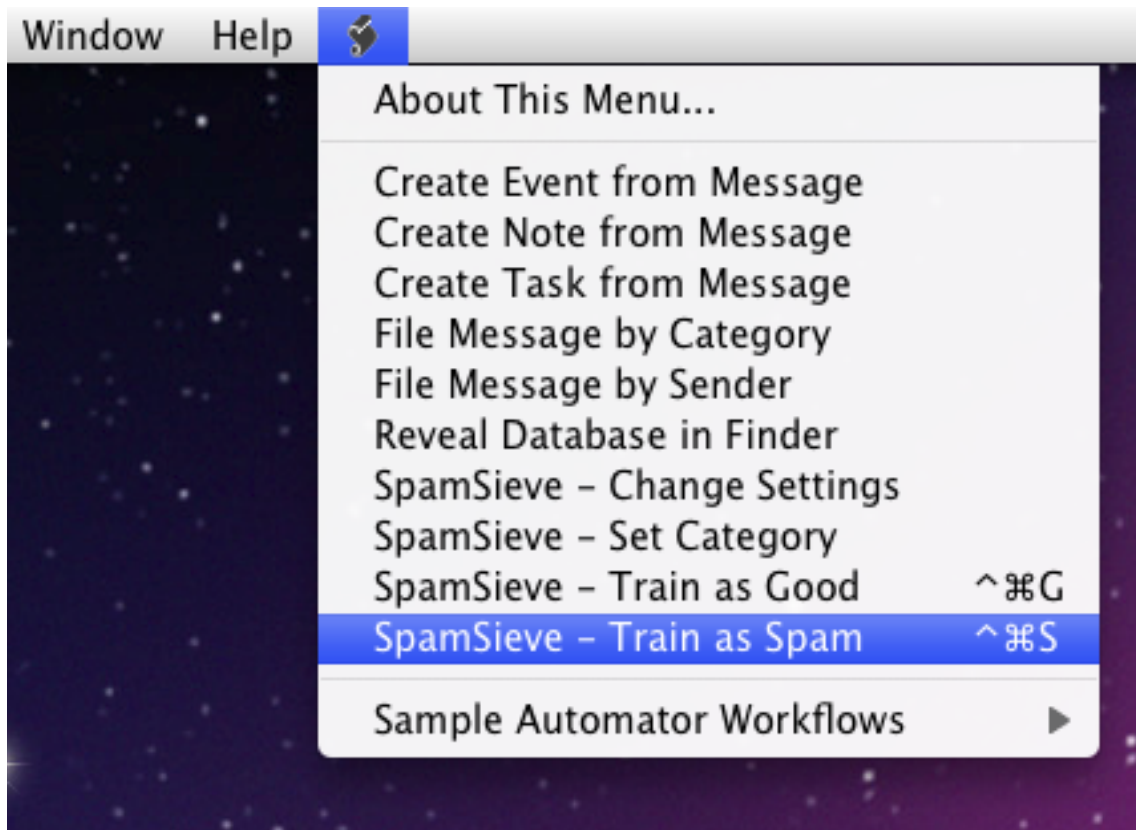
1. Make sure that you are using MailForge 2.0.4 or later.
2. In MailForge's **Junk Mail** preferences, set the **Junk Filtering Strictness** to **Use SpamSieve**.
3. In MailForge's **Accounts** preferences, make sure that **Full Email** is checked for each IMAP account.
4. Now proceed to the [Do an Initial Training](#) section.
  - To train SpamSieve with spam messages, select the messages, go to MailForge's **Message** menu, and choose **Junk**.
  - To train SpamSieve with good messages, select the messages, go to MailForge's **Message** menu, and choose **Not Junk**.

## 8.5 Setting Up Outlook 2011

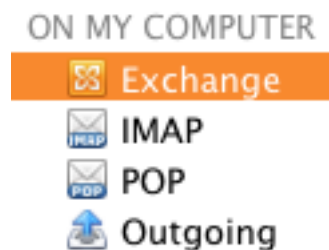
These instructions apply to Outlook 2011 (14.x), from Microsoft Office 2011. If you are using Outlook 365 (also known as Outlook 2016 and 2019, versions 15.x and 16.x), please see the [Setting Up Outlook](#) section. If you are using Microsoft Entourage, please see the [Setting Up Entourage](#) section.

1. Go to Outlook's **Tools** menu and choose **Junk E-mail Protection...** Turn off Outlook's junk filter by clicking **None** and then **OK**.
2. Switch to SpamSieve by clicking on its icon in the Dock. Go to the **SpamSieve** menu and choose **Preferences...** Make sure that [Use Entourage/Outlook address book](#) is checked and click the **Load** button, then the **Outlook** button.

3. Choose **Install Outlook Scripts** from the **SpamSieve** menu. After you quit and re-launch Outlook, you should see four SpamSieve items in Outlook's **Scripts** menu:



4. Choose **Rules...** from Outlook's **Tools** menu. Click on the source list item under **On My Computer** corresponding to the type of account you that have (e.g. POP, IMAP, or Exchange). Ignore the **Exchange Server** section of the window, if any.

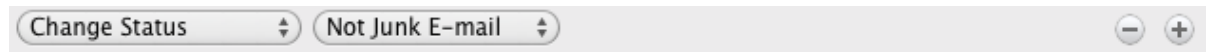


5. If you have more than one kind of account, you will need to repeat Steps 4-6 for each account type.
  - a) If you had previously used SpamSieve with Microsoft Entourage, delete any SpamSieve rules that Outlook brought over from your Entourage setup.
  - b) Click the + button. Change the name of the rule to **SpamSieve - Set Category**.
  - c) For a POP account:

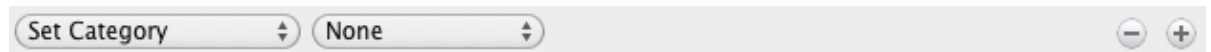
1. Under **When a new message arrives** it should say **All Messages**.

For an IMAP or Exchange account:

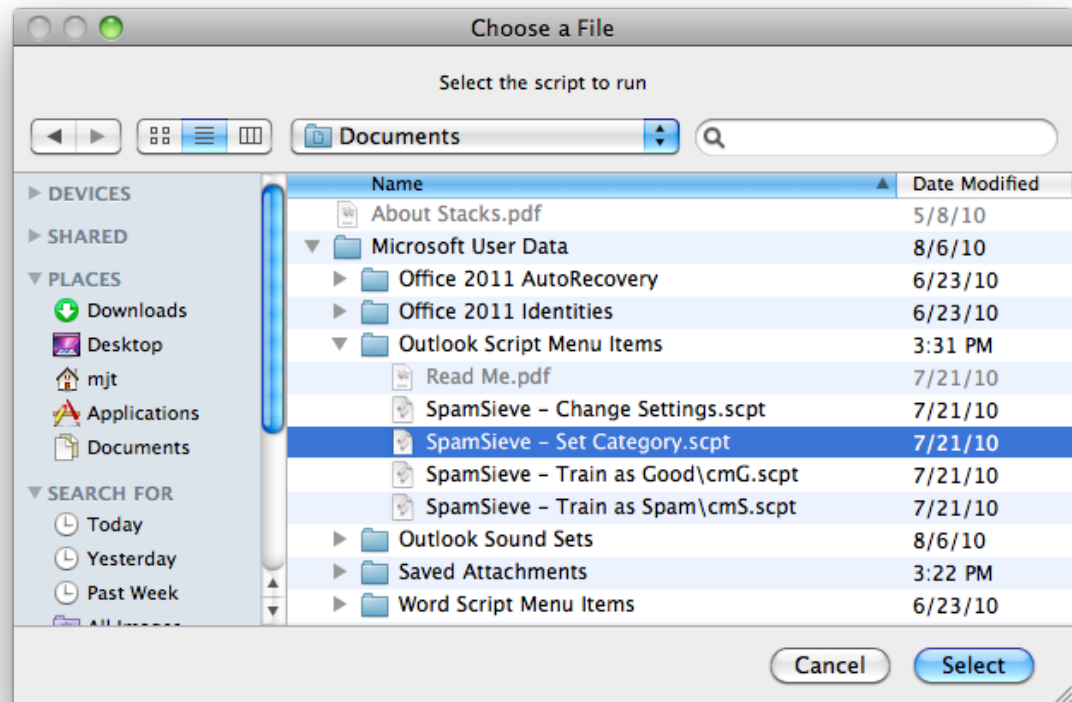
1. Under **When a new message arrives** it should say **Folder Is INBOX (<Account Name>)**.
  2. When you create a new IMAP rule, the pop-up menu at the left will automatically say **Folder**; when you create new Exchange rule, the pop-up menu will say **From** and you will have to change it to **Folder**.
  3. Next, you need to choose the inbox from the pop-up menu at the right. You may have to choose **Choose Folder...** and type “in” to be able to select the inbox.
  4. Click the + button to add an additional rule condition for each IMAP/Exchange account that you have. Change the pop-up menus to say **Folder Is INBOX (<Account Name>)** as before.
  5. Click on **If all conditions are met** and change it to **If any conditions are met**.
- d) Under **Do the following**, click on the - button to the right of **Change status** and **Not Junk E-mail** to delete the **Change status** action.



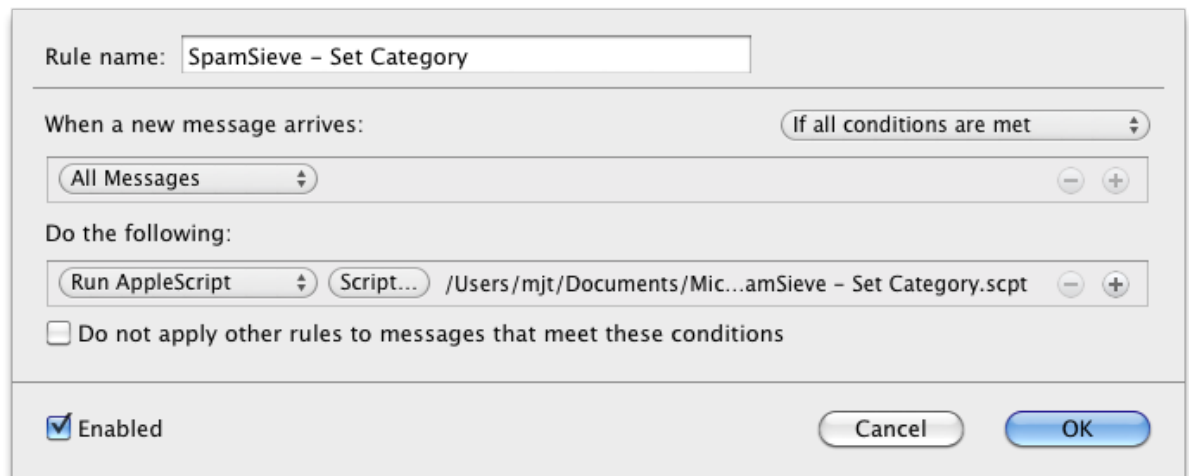
- e) Click on the pop-up menu that says **Set Category** and choose **Run AppleScript**.



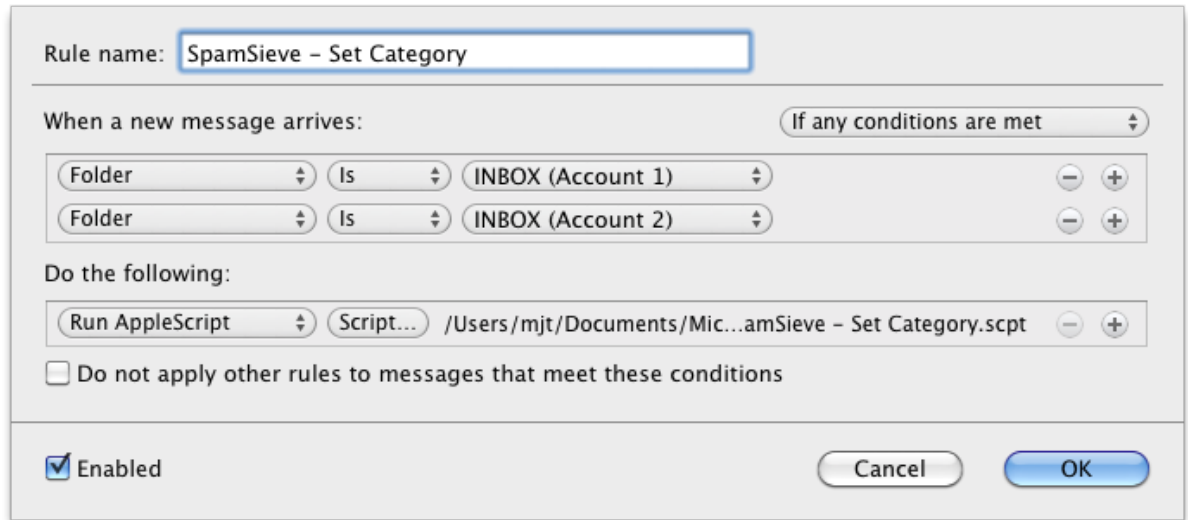
Then click the **Script...** button and **Select** the **SpamSieve - Set Category.scpt** file. This file is stored in the **Outlook Script Menu Items** folder (which is probably inside the **Microsoft User Data** folder inside your **Documents** folder):



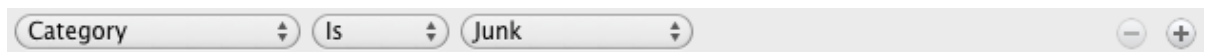
- f) Make sure that **Do not apply other rules...** is unchecked. For a POP account, the rule should now look like this:



For an IMAP or Exchange account, the rule should now look like this:



- g) Click **OK** to close the sheet.
  - h) Drag the **SpamSieve - Set Category** rule to the top of the list.
6. In the **Rules** window, as before, repeat the following steps for each type of account that you have (e.g. POP, IMAP, or Exchange) under “On My Computer”.
- a) Click the + button. Change the name of the rule to **SpamSieve - Move Messages**.
  - b) Under **When a new message arrives**, click on the pop-up menu and change it to say **Category**. Click on the pop-up menu for **None** and change it to **Junk**. The condition should now say **Category Is Junk**.
  - c) Click the + button to the right of **Junk** to make a new condition.

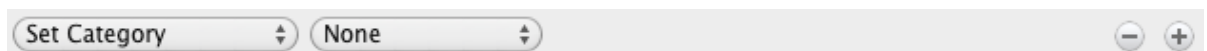


Click on **From** for the new condition and change it to say **Category**. Click on the pop-up menu for **None** and change it to **Uncertain Junk**. The condition should now say **Category Is Uncertain Junk**.

- d) Click on **If all conditions are met** and change it to **If any conditions are met**.
- e) Under **Do the following**, click on the - button to the right of **Not Junk E-mail** to delete the **Change status** action.



- f) Click on the pop-up menu that says **Set Category** and choose **Move Message**.



Change the menu at the right from **None** to **Junk E-mail**. You may have to choose **Choose Folder...** and type “Junk” to be able to select the **Junk E-mail** folder. The rule should now look like:

Rule name:

When a new message arrives: If any conditions are met

|          |    |                |   |   |
|----------|----|----------------|---|---|
| Category | Is | Junk           | - | + |
| Category | Is | Uncertain Junk | - | + |

Do the following:

|              |                           |   |   |
|--------------|---------------------------|---|---|
| Move Message | Junk E-mail (On My Co...) | - | + |
|--------------|---------------------------|---|---|

☒ Do not apply other rules to messages that meet these conditions

☒ Enabled Cancel OK

- g) Click **OK** to close the sheet.
- h) Drag the **SpamSieve - Move Messages** rule so that it is just below the **SpamSieve - Set Category** rule(s) (and above your other rules).

7. Now proceed to the [Do an Initial Training](#) section.

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

The keyboard shortcuts for these commands are Command-Control-S and Command-Control-G.

On macOS 10.14 or later, the first time you try to train a message macOS will ask for [permission to control](#) Outlook and SpamSieve, and you should click **OK**.

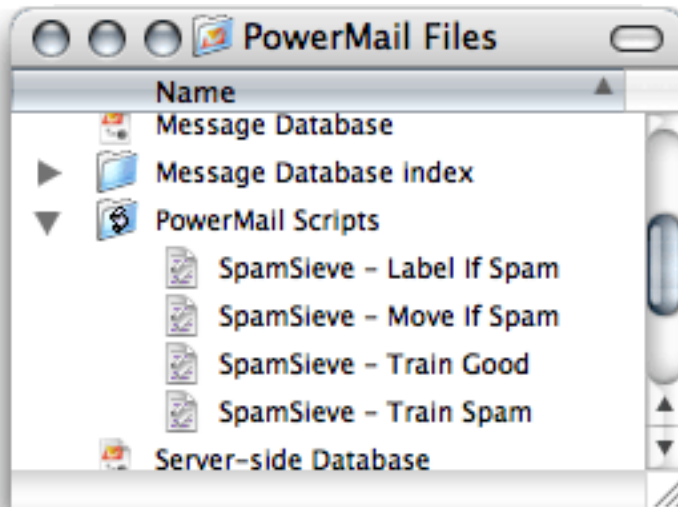
SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **SpamSieve - Set Category** from Outlook's script menu. Then choose **Rules** > **Apply All** from the **Message** menu.

The above is all you need to know about using SpamSieve with Outlook. The [Outlook Customization](#) section explains some more advanced setup options.

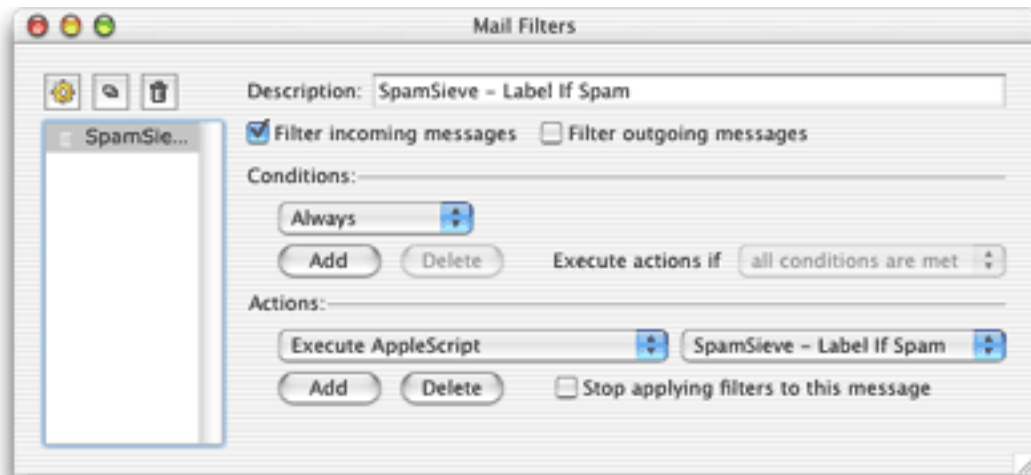
If you need to troubleshoot SpamSieve and Outlook, see the [Checking the Outlook 2011 Setup](#) section.

## 8.6 Setting Up PowerMail 4

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.
4. Now proceed to the [Do an Initial Training](#) section. 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.

SpamSieve will process new mail automatically. If you ever need to manually ask it to sift through a mix of spam and good messages, select the messages and choose **SpamSieve - Label If Spam** or **SpamSieve - Move If Spam** from PowerMail's **Scripts** menu.

## 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.

# 9 Legal Stuff

## Copyright and Trademarks

SpamSieve and this manual are copyright © 2002–2021 by [C-Command Software, LLC](#)<sup>113</sup>. All rights reserved.

SpamSieve is a trademark of C-Command Software, LLC. Mac is a registered trademark of Apple Computer. All other products mentioned are trademarks of their respective owners.

## End User License Agreement

CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT. YOU ACCEPT AND AGREE TO BE BOUND BY THIS LICENSE AGREEMENT BY DOWNLOADING AND INSTALLING THE PROGRAM. IF YOU DO NOT AGREE TO THIS LICENSE, THEN DO NOT DOWNLOAD AND INSTALL THE PROGRAM, AND REMOVE THE SOFTWARE FROM YOUR COMPUTER.

### *License Grant*

“You” means the person or company who is being licensed to use the Software or Documentation. “We,” “us” and “our” means C-Command Software, LLC.

We hereby grant you a nonexclusive license to use one copy of the Software on any single computer, or on multiple computers only used by a single person. The Software is “in use” on a computer when it is loaded into temporary memory (RAM) or installed into the permanent memory of a computer—for example, a hard disk or other storage device.

### *Title*

We remain the owner of all right, title and interest in the Software and related explanatory written materials (“Documentation”).

### *Archival or Backup Copies*

You may copy the Software for backup and archival purposes, provided that the original and each copy is kept in your possession and that your installation and use of the Software does not exceed that allowed in the “License Grant” section above.

### *Things You May Not Do*

The Software and Documentation are protected by United States copyright laws and international treaties. You must treat the Software and Documentation like any other copyrighted material—for example, a book. You may not:

---

<sup>113</sup><mailto:mjt@c-command.com>



- copy the Documentation,
- copy the Software except to make archival or backup copies as provided above,
- sublicense, rent, lease or lend any portion of the Software or Documentation.

### *Transfers*

You may transfer all your rights to use the Software and Documentation to another person or legal entity provided you transfer this Agreement, the Software and Documentation, including all copies, updates and prior versions to such person or entity and that you retain no copies, including copies stored on computer.

### *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. No employee, agent, dealer or distributor of ours is authorized to modify this limited warranty, nor to make any additional warranties.

### *Term and Termination*

This license agreement takes effect upon your use of the software and remains effective until terminated. You may terminate it at any time by destroying all copies of the Software and Documentation in your possession. It will also automatically terminate if you fail to comply with any term or condition of this license agreement. You agree on termination of this license to destroy all copies of the Software and Documentation in your possession.

### *General Provisions*

1. This written license agreement is the exclusive agreement between you and us concerning the Software and Documentation and supersedes any prior purchase order, communication, advertising or representation concerning the Software.
2. This license agreement may be modified only by a writing signed by you and us.
3. This license agreement is governed by the laws of the State of New Hampshire.
4. You agree that the Software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations.

## **Components**

The following open-source components are used in SpamSieve:

- Regular expression support is provided by the [PCRE](http://www.pcre.org)<sup>114</sup> library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

---

<sup>114</sup><http://www.pcre.org>

- [Core Foundation](#)<sup>115</sup> is available under the terms of the [Apple Public Source License](#)<sup>116</sup>.
- [CwlDemangle.swift](#) is Copyright © 2017 Matt Gallagher and is available under the [Apache License v2.0 with Runtime Library Exception](#)<sup>117</sup>.
- [easy-ecc](#) (currently [here](#)) is Copyright © 2013 Kenneth MacKay. All rights reserved.

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

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

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 HOLDER 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.

- [GMellipticCurveCrypto](#) is Copyright © 2014 Richard Moore. 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.

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 HOLDER 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.

<sup>115</sup><http://www.opensource.apple.com/source/CF/CF-368.28/>

<sup>116</sup><http://www.opensource.apple.com/license/apsl/>

<sup>117</sup><http://swift.org/LICENSE.txt>

- [Growl](#)<sup>118</sup> 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.

- Thanks to Allan Odgaard for some code snippets that are used in the Software Update installer.
- [EDCommon](#)<sup>119</sup> 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](#)<sup>120</sup> 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.

## 10 Version History

### 2.9.43—February 22, 2021

- Worked around a bug in the forthcoming macOS 11.3 that could cause SpamSieve to crash at launch.
- Improved the following sections of the manual:

---

<sup>118</sup><http://growl.info>

<sup>119</sup><http://www.mulle-kybernetik.com/software/EDFrameworks/download.html#EDCommon>

<sup>120</sup><http://www.mulle-kybernetik.com/software/EDFrameworks/download.html#EDMessage>

- [If Apple Mail Is Running Slowly](#)
- [Resetting Mail’s Private Plug-Ins Folder](#)
- [Security & Privacy Access](#)
- [Setting Up Apple Mail](#)
- The [Use Growl global notification system](#) checkbox is now shown as disabled when Growl is not available, e.g. on Apple Silicon Macs.
- Improved SpamSieve’s debug logging of messages received and processed.

#### 2.9.42—January 20, 2021

- SpamSieve now runs natively on Apple Silicon Macs.
- Worked around a macOS bug that could block communication between Apple Mail or Outlook and SpamSieve on Apple Silicon Macs. This could cause training not to work and/or messages to accumulate in the **InboxSpamSieve** folder.
- SpamSieve now tries to detect if Apple Mail will incorrectly report an “Incompatible Plug-ins Disabled” error on macOS 11 (e.g. when the installed version of the plug-in actually *is* compatible) and explains how to fix this.
- Improved the following sections of the manual:
  - [If SpamSieve Tells You the Apple Mail Plug-In Isn’t Loading, But It Is](#)
  - [If the Apple Mail Plug-In Doesn’t Appear in the List or Doesn’t Stay Enabled](#)
  - [Resetting Mail’s Private Plug-Ins Folder](#)
  - [Security & Privacy Access](#)
- SpamSieve now maintains its own error log files, so you can still access information for troubleshooting when the macOS system log isn’t working properly.
- Improved the installer and diagnostic report to better work around problems with Apple Mail’s plug-ins folder on macOS 11.
- The software updater reports a more useful error message if you try to update SpamSieve while running it from the disk image. This should prevent confusion where you continue running an old version despite telling it to update.
- The [Apple Mail - Move If Spam](#) script now lets you set a server spam mailbox name via the user defaults without having to edit the script.

#### 2.9.41—December 11, 2020

- Added support for Apple Mail on the forthcoming macOS 11.1. We recommend [updating SpamSieve](#) before updating to macOS 11.1. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#) and [enable the plug-in](#).
- The Apple Mail installer is better able to detect when a new version of macOS requires a new version of SpamSieve.
- Apple Mail is faster at launching SpamSieve and more likely to find the right installed copy of it.
- Worked around a macOS 11 bug that prevented the diagnostic report from working properly on Apple Silicon Macs.
- Worked around a macOS 11 bug that could cause an Apple Mail hang when SpamSieve and Small Cubed MailSuite were both in use.
- Made various changes to try to work around a problem where Apple Mail training commands were intermittently not received on Macs with Apple Silicon.

- Improved the diagnostic report on macOS 11.
- Update the Korean localization.

## 2.9.40—October 19, 2020

- Added support for Apple Mail on the forthcoming macOS 11.0 Big Sur. We recommend [updating SpamSieve](#) before updating to Big Sur. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#) and [enable the plug-in](#).
- Made various changes to improve SpamSieve's filtering accuracy.
- SpamSieve now works with Apple Mail when running on an Apple Silicon Mac.
- On macOS 11, you can now hold down the Option key when installing SpamSieve's Apple Mail plug-in to clear out any active plug-in files that may be preventing Mail from loading the plug-in. (Other third-party Mail plug-ins will be disabled but not deleted; they can be re-enabled using the **Manage Plug-in...** button in Mail's preferences.) This is much easier than the former method on macOS 10.14 and 10.15 that required temporarily disabling SIP.
- Restored Web bug protection in Apple Mail on macOS 11 since it seems to fix the issue in macOS 10.15 that necessitated disabling it.
- The Apple Mail plug-in now has a stapled notarization ticket so that it can be loaded even if the Mac can't contact Apple's notarization servers.
- The Apple Mail plug-in installer is better at working around macOS quarantine bugs.
- It is now possible to [save a diagnostic report](#) when SpamSieve's Dock icon is hidden (and thus the **Help** menu is inaccessible) by clicking a [special link](#)<sup>121</sup>.
- Improved the following sections of the manual:
  - [Checking the Airmail Setup](#)
  - [Enabling and Updating the Apple Mail Plug-In](#)
  - [If Apple Mail Is Running Slowly](#)
  - [If the Apple Mail Plug-In Doesn't Appear in the List or Doesn't Stay Enabled](#)
  - [Outlook IMAP/Exchange Account Rules](#)
  - [Setting Up Apple Mail](#)
  - [Setting Up Gmail, iCloud, Yahoo, AOL, or Other Web Mail](#)
  - [Using a Spam Mailbox on the Server](#)
  - [Why does a message disappear or go back to the spam mailbox after I train it as good?](#)
- The [Setting Up Outlook](#) section of the manual now explains that you should turn off the **New Outlook** switch because it [does not support AppleScript](#).
- SpamSieve now requires macOS 10.9 or later.
- Improved the diagnostic report.
- If a duplicate Apple Mail plug-in is installed, SpamSieve now reveals it to you in Finder.
- The Apple Mail installer is better at reporting when the loaded version of the plug-in is different from the installed version, to help track down [data vaults problems](#).
- Added a workaround for a macOS privacy performance bug.
- Fixed a regression where SpamSieve would unnecessarily update its Mail plug-in at each launch.
- If an icon file is damaged, the error message now suggests installing a fresh copy of SpamSieve.

---

<sup>121</sup>`x-spamsieve://diagnosticReport`

- Fixed a bug where the text of an Apple Mail installer alert wasn't accurate if you had relocated your Mac's home folder.
- Fixed a bug where the tags field was inappropriately shown.

## 2.9.39—March 4, 2020

- Made various changes to improve SpamSieve's filtering accuracy.
- When you select spam messages in Apple Mail, the message list text is more readable through a variety of highlight colors.
- Improved the following sections of the manual:
  - [How can I copy my training data to another machine?](#)
  - [If the Apple Mail Plug-In Doesn't Appear in the List or Doesn't Stay Enabled](#)
  - [Setting Up Airmail](#)
  - [Setting Up an Apple Mail Drone](#)
  - [Turning Off the Fastmail Spam Filter](#)
  - [Why are messages marked as spam in Apple Mail but not moved?](#)
- Added the [Processing Messages Before SpamSieve](#) and [Setting Up Airmail 1–3](#) sections of the manual.
- Worked around a change in the forthcoming macOS 10.15.4 that could prevent Mail from loading SpamSieve's plug-in if you had relocated your home folder to another volume. If Mail reports an error loading the plug-in, choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#) to update it.
- Worked around an Apple Mail bug that could, in rare cases on macOS 10.15, cause spam messages to be marked as spam but not moved to the **Spam** mailbox. If this is happening for you, choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#) to enable the workaround.
- A small percentage of Apple Mail users are seeing a macOS 10.15 bug where a rule that is supposed to move messages to an IMAP or Exchange mailbox instead deletes them. If this is happening for you, make sure that your **SpamSieve** rule is set to move the messages to a local mailbox under **On My Mac** (as recommended in the [Setting up Apple Mail](#) section of the manual) rather than to a mailbox on the mail server.
- A small percentage of Apple Mail users are seeing a macOS 10.15 bug where moving a message to an IMAP or Exchange mailbox (either via drag-and-drop or via AppleScript, as SpamSieve does) instead deletes it. If this is happening for you, you can use the [Change Settings](#) command to set SpamSieve to (a) move messages trained as spam to a local **Spam** mailbox (this is the default); and (b) not *move* messages trained as good back to the inbox (you can instead *copy* them by Option-dragging or using the menu command).
- SpamSieve now includes an experimental feature to save backup copies of the messages that it has processed. This can help prevent data loss if you are one of the unlucky users affected by a bug in the macOS 10.15 version of Apple Mail that can delete messages when moving them from one mailbox to another. The bug is not actually related to SpamSieve and also manifests when it's not installed. However, training messages with SpamSieve is a common reason that Mail would be asked to move messages, possibly triggering the bug. And since SpamSieve sees the messages, anyway, it's in a good position to help mitigate the bug. For more information about backups and how to enable them, please see the [Backing Up Messages](#) section of the manual.
- If you are running into a bug in macOS 10.15 where Mail hangs for 10+ seconds during launch, the [If Apple Mail Is Running Slowly](#) section of the manual now describes how you can work around this by disabling and re-enabling SpamSieve's plug-in.

- Worked around an Apple Mail bug that could cause the **Preferences** window to be blank on macOS 10.15, making it impossible to enable SpamSieve's plug-in or to access other Mail settings.
- When installing the Apple Mail plug-in, SpamSieve will now warn you if Mail's files are stored on a different volume than your home folder, which would prevent Mail from loading the plug-in on macOS 10.14 or later.
- If SpamSieve detects that macOS's AppleScript system files are damaged, which can prevent training from working, it will now recommend that you reinstall macOS.
- After installing the Apple Mail plug-in, we recommend clicking the **Quit and Show Instructions** button. If you opt not to do this, the other button is now titled **Continue** rather than **Cancel**, to better reflect that the plug-in has still been installed and still needs to be enabled.
- There's now an esoteric preference to mark Outlook messages as unread after filtering, to work around a mysterious issue where moving a message to another folder caused it to be marked as read.
- SpamSieve now logs to Console to help you detect inefficient regexes that slow down rule matching.
- Revised the Apple Mail and Postbox plug-ins for new macOS notarization requirements.
- Fixed a bug where training a message as good in Apple Mail could switch to *displaying* the inbox instead of *moving* the message to the inbox.
- Fixed a bug where SpamSieve could warn you that the Apple Mail plug-in was not enabled if Mail relaunched while SpamSieve was in the process of uninstalling.
- Fixed a bug where relaunching Apple Mail while SpamSieve was reminding you to enable the plug-in could result in a duplicate alert being shown.

### 2.9.38—November 19, 2019

- SpamSieve 2.9.38 (and also 2.9.37) are compatible with macOS 10.15, however a small number of customers are seeing issues with the Catalina version of Apple Mail. The latest information about Catalina is available [here](#).
- Worked around an AppleScript bug in Apple Mail on macOS 10.15 that could result in messages trained as good being moved to the inbox of an account that's disabled, making it look like the messages disappeared. This fix is available for all new installations and for older ones if you choose [Install Apple Mail Plug-In](#) from the **SpamSieve** menu. (If you weren't seeing this problem or have no disabled accounts, it's not necessary to update the plug-in.)
- Worked around an issue that could prevent some Apple Mail messages from being filtered through SpamSieve if SpamSieve had not yet launched and the Mac was overloaded, e.g. because it was relaunching all apps after logging in.
- Worked around a problem where SpamSieve could be slow to launch if the system privacy database was overloaded.
- Added the [If the Apple Mail Plug-In Doesn't Appear in the List or Doesn't Stay Enabled](#) section of the manual.
- Improved the following sections of the manual:
  - [Enabling and Updating the Apple Mail Plug-In](#)
  - [How can I rebuild Apple Mail's database?](#)
  - [Setting Up Apple Mail](#)
  - [Turning Off Microsoft Spam Filters](#)
  - [Why does a message disappear or go back to the spam mailbox after I train it as good?](#)
- A macOS 10.15 bug can prevent Apple Mail messages from being moved to the **Spam** mailbox, leaving them colored as spam in the inbox. SpamSieve now offers an alternate [Apple Mail Script Rule](#) setup for the small number of customers affected by this bug.



- Added an experimental esoteric preference (click to [enable](#)<sup>122</sup>/[disable](#)<sup>123</sup>) to flag incoming spam messages as gray. A few customers are running into a Mail bug in macOS 10.15 that prevents rules from moving messages (even when using an [Apple Mail Script Rule](#)). This workaround makes it possible to set up a smart mailbox for gray flagged messages, so that they can easily be viewed and bulk-deleted even if the messages remain in the inbox.
- Worked around some bugs in macOS 10.15 that could cause Mail to hang when SpamSieve launched.
- If the **Rules** file is damaged, SpamSieve will now report some more information about the problem.
- The [Apple Mail - Server Junk Mailbox](#) script now has an option to only mark confirmed spam messages as read, leaving them in the server spam mailbox rather than moving them to a shared spam mailbox.
- Fixed a bug that could cause a crash when a [Software Update...](#) error occurred.
- Fixed a bug with the crash reporter window and Dark Mode.
- Modernized the localizations.

## 2.9.37—August 19, 2019

- SpamSieve is now compatible with Apple Mail under macOS 10.15 (which is now in beta).
- It's best to update to SpamSieve 2.9.37 now, before updating to macOS 10.15. If you are already using macOS 10.15, the SpamSieve 2.9.36 auto-updater won't work, so you should instead use the **Download** button in the [Software Update...](#) window and install the update manually, according to the instructions in the Read Me file. Once you have SpamSieve 2.9.37, auto-updates on macOS 10.15 will work normally.
- Updated the documentation for macOS 10.15.
- The [Outlook - Filter Mailboxes](#) app is now notarized for compatibility with macOS 10.15. If you've already installed the helper app, it should not be necessary to update it, but this change is needed for future updates as well as new installations.
- Various Apple Mail error messages and documentation are better at reminding you to grant SpamSieve [Full Disk Access](#) when not having that might be the cause of the error, e.g. SpamSieve thinking its plug-in is not loaded.
- Apple Mail on macOS 10.15 has a bug where it will not load plug-ins that are installed in the normal location if you've redirected your home folder to another volume. If SpamSieve detects this situation, it will apply a workaround (moving the plug-in to an alternate location) and show an alert that explains what it's doing.
- Renamed the "Setting Up Outlook 365" section of the manual to [Setting Up Outlook](#), as it covers all current versions of Outlook, not just 365. This section has also been substantially rewritten to make it clearer what to do for each type of account.
- The [Can other Apple Mail plug-ins cause problems with SpamSieve?](#) section of the manual now recommends using Mail's own plug-in manager instead of manipulating the **Bundles** folder directly.
- Fixed a bug where SpamSieve would sometimes ask you to enable an old Apple Mail plug-in (which wasn't possible, because it was old) and quit, where instead it should have offered to update it first.
- Worked around an Apple Mail bug where training a message as good sometimes didn't move it to the inbox because Mail reported a script error when checking whether the account was enabled.

<sup>122</sup>[x-spamsieve://default?k=AppleMailPlugInSetFlagged&v=YES](#)

<sup>123</sup>[x-spamsieve://default?k=AppleMailPlugInSetFlagged&v=NO](#)



- Improved the diagnostic report.
- [Software Update...](#) reports a better error message if it was unable to install the new version of the app.

### 2.9.36—May 24, 2019

- Made various changes to improve SpamSieve’s filtering accuracy.
- When using Outlook 365, you can now use Outlook rules to organize messages into folders, and SpamSieve will filter them (rather than just the messages in the inbox). The details for how to set this up are in **Filtering Other Folders** in the “Setting Up Outlook 365” section of the manual. (This has always worked automatically, with no special setup, in previous versions of Outlook and in Apple Mail.)
- After you manually refilter messages in Outlook, SpamSieve now clears the selection to prevent accidental bulk training when correcting a spam message that remains.
- Fixed a problem where some Apple Mail messages that were colored as spam still displayed with white text in Dark Mode, which was difficult to read.
- Improved the following sections of the manual:
  - [Does SpamSieve stop Web bugs?](#)
  - [How can I hide SpamSieve’s Dock icon?](#)
  - [Security & Privacy Access](#)
  - [Setting Up Airmail](#)
  - [Why do Apple Mail messages bounce back to the inbox after I train them as spam?](#)
- If SpamSieve encounters an error because your Mac’s storage is full, it now displays information about the free space available and recommends [Apple’s guide](#) to freeing up storage space.
- SpamSieve reports a more useful error message if it determines that the reason its application package is damaged is because it’s running from a Carbon Copy Cloner safety net.
- Improved the error message when uninstalling the Apple Mail plug-in if SpamSieve hasn’t been granted Full Disk Access.
- Improved the error message when SpamSieve doesn’t have access to your Contacts.
- Worked around a problem where asking Apple Mail for the list of mailboxes could cause it to hang at launch.
- When training a good message in Apple Mail, if SpamSieve can’t find the proper inbox it logs more information to help figure out what happened.
- Fixed a bug displaying the number of licenses in the **Purchase** window.
- Fixed a bug where debug logging of messages that caused parser crashes wasn’t working with Apple Mail.
- The diagnostic report now includes information about when the privacy database was last reset.
- Diagnostic reports now work better when SpamSieve lacks Full Disk Access.
- Updated to Xcode 10.2.

### 2.9.35—December 20, 2018

- Worked around an issue where macOS 10.14 would tell SpamSieve that Mail had finished launching when it hadn’t. If Mail took a long time to launch, this could make SpamSieve erroneously think that its plug-in wasn’t enabled, so it would show some unnecessary and annoying alert windows asking you to fix this.

- SpamSieve no longer updates its Apple Mail plug-in with each new release because this causes extra work to [re-enable](#) it for customers using macOS 10.14. Instead, the plug-in only auto-updates when there is a major change that we recommend for all users. You can still update it manually (by choosing [Install Apple Mail Plug-In](#) from the menu) if you want to ensure that you have the latest version.
- Improved the following sections of the manual:
  - [Enabling and Updating the Apple Mail Plug-In](#)
  - [Security & Privacy Access](#)
  - “Setting Up Outlook 365”
  - [Turning Off the AOL Spam Filter](#)
- Improved SpamSieve’s error handling when trying to uninstall its Apple Mail plug-in while lacking Full Disk Access.
- Fixed a bug where AppleScript permissions errors could report the wrong app name.
- Fixed a bug where some Retina images in the manual were shown at double size.
- Fixed a bug where the help index file was marked as executable.

## 2.9.34—October 30, 2018

- Made a variety of changes to work better with Apple Mail on macOS 10.14:
  - SpamSieve now uses a variety of heuristics to better detect when Mail has finished launching before checking that its plug-in is enabled. This helps avoid annoying dialogs and prevents unnecessary rule deactivations if Mail takes a really long time to launch, e.g. on a slower Mac that has rebooted and is restoring all the previously open applications at once or if a utility such as iLock has halted Mail during the launch process.
  - SpamSieve can now protect you from a disabled plug-in when Mail launches after SpamSieve launches, e.g. if you are using SpamSieve with multiple mail clients and so SpamSieve is not always launched as a result of Mail launching.
  - SpamSieve now detects and repairs problems with Mail’s preferences folder that could prevent Mail from showing the **Manage Plug-ins...** button.
  - If macOS has forgotten that you gave SpamSieve [Full Disk Access](#), SpamSieve will now detect this and remind you to grant it again.
  - If SpamSieve can’t install its Mail plug-in because it doesn’t have [Full Disk Access](#), it no longer suggests that you install the plug-in manually. (It is better for you to grant access and then try the automatic installer again.)
  - If you’ve previously declined to give SpamSieve [Automation access](#) to control Mail, SpamSieve will now remind you to do this (and open System Preferences for you) when you try to train a message, instead of failing silently.
  - The [Apple Mail - Remote Training](#) and [Apple Mail - Server Junk Mailbox](#) scripts, when running as standalone applications, now explain to you that they need [Automation access](#) in order to function.
  - Adjusted the launch agent so that SpamSieve more reliably launches when Mail launches, and sandbox errors aren’t logged to Console.
  - Since version 2.9.21, SpamSieve has overridden the text color in Mail’s message list in order to improve the contrast and readability for spam messages that are marked with a [colored background](#). This now works on macOS 10.14, including with Dark Mode.
  - The `AppleMailAllJunkMessagesUseBlackText` esoteric preference now switches the color for Dark Mode on macOS 10.14.
  - SpamSieve now logs more information to Console and diagnostic reports to help diagnose problems with the Mail plug-in.

- The alert and manual now clarify that, if you no longer want to use SpamSieve with Mail, you can prevent SpamSieve from reminding you to enable the plug-in by [uninstalling it](#).
- SpamSieve no longer wastes time waiting for Mail to launch when there are no rules for it to reactivate, anyway.
- Fixed an error reporting bug when activating the Mail rules.
- Fixed a bug where a fresh install on macOS 10.14 wouldn't remember that the Mail plug-in had been installed.
- [Outlook Filter Mailboxes](#) now shows a more helpful error message if it lacks [Automation access](#) on macOS 10.14.
- Due to [changes](#) in Airmail and macOS 10.14, Airmail versions 3.6.3 through 3.6.41 are not compatible with SpamSieve when using macOS 10.14. You should use Airmail 3.6.42 or later.
- When [checking the setup](#) for your e-mail client, the instructions now recommend verifying that [Automation access](#) has been granted.
- The [Apple Mail - Discard Spam](#) script reports a better error if Mail times out because there were too many messages in the trash.
- Updated the [Security & Privacy Access](#) section of the manual.
- The **About** window now includes a link to the privacy policy and has an updated layout.
- Updated SpamSieve's code signing for the latest Apple notarization requirements.
- Fixed a bug where training a message as spam in Apple Mail would display the **Spam** mailbox instead of moving the message if you were using the [old GUI scripting workaround](#) on macOS 10.12 or later with a non-US localization.
- Fixed a bug where SpamSieve could get confused by the presence of Fluid App instances.

### 2.9.33—September 21, 2018

- Streamlined the flow of using SpamSieve with Apple Mail on macOS 10.14. SpamSieve does a better job of guiding you through the Mojave security changes to make setup as easy as possible. For the smoothest experience, we recommend updating to SpamSieve 2.9.33 before you update your Mac to macOS 10.14.
- On macOS 10.14, it is possible for an Apple Mail plug-in to be installed but not yet enabled. When SpamSieve's plug-in is not enabled, the SpamSieve rule(s) in Mail cannot function properly and may move new good messages to the spam mailbox [without consulting SpamSieve](#). SpamSieve now protects you from this by automatically deactivating the rules if it notices that the plug-in is disabled. Once you've [enabled the plug-in](#), it reactivates the rule(s) for you.  
For completeness, we mention that there is a chance that Mail will move some messages before SpamSieve can deactivate the rule(s), e.g. because Mail downloaded them while SpamSieve was launching or because you declined when SpamSieve requested access to control Mail. If you end up with some good messages in the spam mailbox that are uncolored (because Mail moved them without consulting SpamSieve), you can just drag them back to your inbox.  
If you want to fully prevent messages from being moved to the spam mailbox, you can manually deactivate (uncheck) the SpamSieve rule(s) in Mail's preferences until you know that the plug-in is loaded (i.e. you see the SpamSieve menu commands in Mail's **Message** menu). However, most users will find it easier to let SpamSieve manage the rule(s) for them.
- If you have previously used SpamSieve with Apple Mail but are now using a different mail client, you can choose [Uninstall Apple Mail Plug-In...](#) from the **SpamSieve** menu in order to prevent SpamSieve from reminding you to enable the Mail plug-in.
- If the [Uninstall Apple Mail Plug-In...](#) command can't remove the Mail rules because it lacks **Automation** access on macOS 10.14, it will now proceed with uninstalling the other items and ask you to remove the rules manually rather than stopping with an error.

- SpamSieve now supports the Hardened Runtime on macOS 10.14.
- SpamSieve is now notarized by Apple.
- The former “Advanced Outlook Setup for Large Inboxes” (which uses the **InboxSpamSieve** folder) is now the standard setup described in the “Setting Up Outlook 365” section of the manual. This setup makes Outlook more responsive and provides for more accurate filtering when setting up SpamSieve for the first time. If you are already successfully using Outlook 365 with SpamSieve, the old setup is still supported, so you don’t have to change anything.
- Improved the following sections of the manual:
  - [Enabling and Updating the Apple Mail Plug-In](#)
  - [Security & Privacy Access](#)
  - [Setting Up MailMate](#)
  - “Setting Up Outlook 365”
  - [Turning Off the Gmail Spam Filter](#)
- Reduced the sizes of some large screenshots in the HTML manual so that the text is more easily readable.
- Fixed a bug where some screenshots in the PDF manual were displayed at double size instead of at Retina resolution.
- Removed support for legacy mail clients that no longer work on SpamSieve’s supported macOS versions: Claris EMailer, Eudora, Outlook Express, and Thunderbird 2.x.

### 2.9.32—August 30, 2018

- SpamSieve now supports macOS 10.14 Mojave and Dark Mode.
- Made various changes to improve SpamSieve’s filtering accuracy.
- Apple Mail
  - SpamSieve is now compatible with Apple Mail under macOS 10.14. It’s easiest if you [update](#) to SpamSieve 2.9.32 [before](#) updating to 10.14. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
  - macOS 10.14 adds some security protections for Apple Mail, and so you will need confirm to the system that you want SpamSieve to be able to access Mail and that you want Mail to load SpamSieve’s plug-in. SpamSieve will automatically advise you of what you need to do and when, but the steps are included here for reference:
    - \* In order to install the Mail plug-in, you’ll need to give SpamSieve **Full Disk Access** using System Preferences. This is described in the [Security & Privacy Access](#) section of the manual.
    - \* In order for Mail to load SpamSieve’s plug-in, you’ll need to enable it in Mail’s preferences. This is described in the [Enabling and Updating the Apple Mail Plug-In](#) section of the manual.
    - \* Each new version of SpamSieve will auto-update the installed plug-in, but you will need to re-enable it in Mail’s preferences. If the plug-in is installed but not enabled, Mail will move new messages to the **Spam** mailbox without consulting SpamSieve. You can prevent this by temporarily disabling (unchecking) the **SpamSieve** rule in Mail’s preferences before updating SpamSieve. Or you can just drag the messages back to the inbox if you happen to receive any before you’ve had a chance to re-enable the plug-in.
    - \* In order to train messages in Mail, SpamSieve needs **Automation** access to control Mail. When macOS asks if SpamSieve should be able to control Mail, you should click **OK**. This is described in the [Security & Privacy Access](#) section of the manual.

- The [Software Update...](#) command now advises you about re-enabling SpamSieve’s Mail plug-in after the update if you are using macOS 10.14.
- Added the [Keeping Spam Messages Out of Gmail’s Archive](#) section of the manual.
- If Mail can’t find the SpamSieve application file, e.g. because you manually deleted it in attempting to uninstall manually, it now offers the option of uninstalling the SpamSieve plug-in for you, so that you don’t have to reinstall the app to use the automatic installer.
- If SpamSieve doesn’t have **Full Disk Access**, it will now log a single error to that affect, rather than a flood of file permissions errors.
- SpamSieve now detects if the installed plug-in is up-to-date but not enabled (macOS 10.14–only) in Mail and will explain how to fix this.
- Fixed a problem where [color-specific](#) rules didn’t apply their actions on macOS 10.14.
- The [Apple Mail - SaneBox](#) script is better at handling and reporting errors.
- The Mail plug-in is no longer code-signed, to work around an issue with macOS 10.14, and thus SpamSieve no longer checks whether it’s damaged.
- Fixed a bug where the Mail plug-in could show the same error message repeatedly if the SpamSieve application was deleted, thus interfering with access to Mail itself.
- Fixed a typo in Mail debug logging.
- Microsoft Outlook 365
  - Added support for Outlook 365’s new kind of Gmail accounts that show up as “Google” accounts rather than as “IMAP” accounts.
  - Filtering is faster and will now process any messages in the **InboxSpamSieve** folder, even read ones.
  - SpamSieve is better able to recover when Outlook reports an error getting a message’s account.
  - To get these improvements, please go to the “Setting Up Outlook 365” section of the manual and follow the instructions in Step 6 to update your copy of **Outlook - Filter Mailboxes.app**.
  - The **Advanced Outlook Setup for Large Inboxes** section of the manual now describes a different way to do the setup if you are using Outlook 16.17 (currently available on the Office Insider track) with a Gmail account.
  - Fixed a bug where SpamSieve would incorrectly log that the Outlook scripts were damaged if you were using Outlook 365 but had previously used Outlook 2011 and still had its old scripts installed at the old location.
- Added the [Setting Up Other Mail Clients](#) section of the manual.
- Improved the following sections of the manual:
  - “Checking the Outlook 365 Setup”
  - [Install Apple Mail Plug-In](#)
  - [Setting Up Apple Mail](#)
  - “Setting Up Outlook 365”
  - [Turning Off Microsoft Spam Filters](#)
  - [Turning Off the AOL Spam Filter](#)
  - [Turning Off the Gmail Spam Filter](#)
  - [Turning Off the Yahoo Mail Spam Filter](#)
  - [Uninstalling SpamSieve](#)
  - [Why does SpamSieve always need an update when macOS is updated?](#)
- When you click the link to show SpamSieve’s Dock icon, the change now takes effect immediately, as quitting and relaunching to see the effect was difficult to do when the Dock icon was hidden.

- Added a **statistics report** AppleScript property, which is a string with the current contents of the **Statistics** window.
- The **Copy Stats** button no longer copies zeroes to the clipboard when the statistics haven't been calculated yet.
- Worked around a bug in macOS 10.13 that could prevent the log file from being written.
- Worked around a macOS 10.13 bug that could prevent keyboard input after closing the **Help** menu.
- Worked around a bug in macOS 10.13.4 that could cause an internal error when locating SpamSieve's data files.
- An error saving the system log for the diagnostic report is no longer fatal, so other files can still be saved to the report.
- Fixed a bug where holding down the Command and Option keys to reset one of SpamSieve's damaged files didn't work if the file was seriously damaged.
- Fixed a spurious error message when trying to launch SpamSieve if it was already running.

### 2.9.31—April 30, 2018

- Made various changes to improve SpamSieve's filtering accuracy.
- Fixed a database bug that could cause SpamSieve to crash when processing a particular type of spam message containing garbage Unicode characters in the subject.
- [Outlook - Filter Mailboxes](#) now checks for new inbox messages every 1 minute by default (instead of 5), is more efficient, and is able to filter inboxes with localized names that were previously ignored.
- Updated the [Requirements](#) and [Setting Up Postbox](#) sections of the manual. Postbox 6 no longer supports plug-ins, so we recommend continuing to use Postbox 5 for the time being or using the Apple Mail drone setup in the background.
- The Outlook sections of the manual have been renamed to “Setting Up Outlook 365” and [Setting Up Outlook 2011](#) for clarity.
- Improved the following sections of the manual:
  - [Automatically Deleting Old Spam Messages](#)
  - [Checking the Apple Mail Setup](#)
  - [Setting Up MailMate](#)
  - [Using a Spam Mailbox on the Server](#)
- Worked around a bug in macOS 10.13 that could cause an internal error at launch when resolving an alias.
- The [Apple Mail - Discard Spam](#) script is better able to work around Mail slowness that could leave spam messages stranded in the trash.
- Diagnostic reports now include more information about localizations and SpamSieve helper processes.
- Made various minor code updates.
- Fixed a crash reporter bug that could prevent some information from being logged.

### 2.9.30—January 30, 2018

- SpamSieve is now 64-bit only and requires macOS 10.7 or later.
- Made various changes to improve SpamSieve's filtering accuracy.

- You can now click the [Outlook - Filter Mailboxes](#) icon in the Dock to make it filter the new inbox messages immediately instead of waiting until the next scheduled check.
- The [Apple Mail - Remote Training](#) script now auto-creates the **TrainGood** and **TrainSpam** mailboxes for you.
- Added the [Apple Mail - Block Sender](#) script.
- Improved the following sections of the manual:
  - “Checking the Outlook 365 Setup”
  - [Only Filtering Certain Accounts](#)
  - [Setting Up Apple Mail](#)
- SpamSieve can now recover from certain types of damage to a **Rules** file by logging information about the damaged rules and modifying them so that they don’t cause crashes.
- Manually installing the Apple Mail plug-in now forces creation of a new launch agent **.plist** file, even if nothing has changed, to work around a problem with it not loading.
- The [Apple Mail - Remote Training](#), [Apple Mail - SaneBox](#), and [Apple Mail - Server Junk Mailbox](#) scripts work around a macOS bug that reports that System Events is not running.
- **Outlook - Filter Mailboxes** now works around an Outlook bug with getting folders by name.
- Improved the error reporting when a file cannot be written.
- Fixed a bug where SpamSieve could be fooled into parsing the wrong e-mail address out of a message header ([Mailsploit](#)).
- Fixed a bug where a misleading error message would be presented if a secure connection could not be made to the software update server.
- Fixed a spurious error in diagnostic reports on macOS 10.12 and later.
- Made various code modernizations.
- Updated the German localization.

## 2.9.29—August 24, 2017

- Works with Apple Mail under macOS 10.13 High Sierra (currently in beta). It’s easiest if you [update](#) to SpamSieve 2.9.29 [before](#) updating to 10.13. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- To get the improvements (described below) to SpamSieve’s integration with Microsoft Outlook 2016, please follow these instructions after updating SpamSieve:
  1. Quit **Microsoft Outlook** and **Outlook - Filter Mailboxes**.
  2. From [the SpamSieve menu](#) in **SpamSieve**, choose [Install Outlook Scripts](#).
  3. Go to the “Setting Up Outlook 365” section of the manual and follow the instructions in Step 6 to update your copy of **Outlook - Filter Mailboxes.app**.
- Made various changes to improve SpamSieve’s filtering accuracy.
- Made various improvements to the [Outlook - Filter Mailboxes](#) app for Microsoft Outlook 2016:
  - The “Setting Up Outlook 365” section of the manual has been updated to be more complete and clear.
  - Worked around a hang in Outlook when there are lots of messages in the inbox.
  - There is an optional “Large Inboxes” setup that can greatly speed up the processing of new messages if you have lots of old messages in your inbox.



- Filtering now works when the Mac is running in Dutch or Swedish.
- It is now possible to configure the options using [esoteric preferences links](#), so that you don't have to edit the script itself.
- Improved the debug logging and error reporting.
- Worked around a bug in Microsoft Outlook 15.36 where it could incorrectly report that no messages were selected, thus preventing training from working.
- The [Apple Mail - Remote Training](#) script now sets and clears message background colors and (optionally) flags. This way if a server filter and SpamSieve share the same **Spam** mailbox, you can easily see which messages are confirmed as spam by SpamSieve because they will be marked in its normal way.
- Improved the following sections of the manual:
  - “Checking the Outlook 365 Setup”
  - [Converting Your Apple Mail Setup to IMAP](#)
  - [Requirements](#)
  - [Setting Up GyazMail](#)
  - “Setting Up Outlook 365”
  - [Turning Off the AOL Spam Filter](#)
  - [Turning Off the Fastmail Spam Filter](#)
  - [Turning Off the Gmail Spam Filter](#)
  - [Uninstalling SpamSieve](#)
- Improved the scrolling speed in the **Blocklist**, **Corpus**, and **Whitelist** windows.
- The diagnostic reporter can now check whether the application package is damaged
- SpamSieve is better at detecting and reporting problems with the launch agent.
- Logged errors now use indentation to improve readability.
- SpamSieve now fixes the permissions of the log file if it can't append to it (and worked around an OS bug reporting such errors).
- Improved the Apple Mail debug logging.
- Improved the reporting of corpus reset errors.
- Improved the error reporting for damaged files.
- Documentation and **Help** menu links to [c-command.com](#) now use [https](#) instead of [http](#).
- Made various code modernizations.
- Fixed a bug that could cause a -10004 error when filtering messages for Microsoft Outlook 2016.
- Fixed a bug that could cause a crash when processing incoming Apple Mail messages on macOS 10.13.
- Fixed a bug where some **Preferences** window labels were truncated on Mac OS X 10.10 due to OS font changes.

## 2.9.28—February 27, 2017

- Works with Apple Mail under macOS 10.12.4. It's easiest if you [update](#) to SpamSieve 2.9.28 [before](#) updating to 10.12.4. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve's filtering accuracy.



- The **Save Diagnostic Report...** command in the **Help** menu now works with all versions of macOS that SpamSieve supports.
- Improved the following sections of the manual:
  - [How can I open the Library folder?](#)
  - [Requirements](#)
  - [Sending in an Error Report](#)
  - [Sending in Apple Mail Rules](#)
  - [Sending in the SpamSieve Log File](#)
  - [Setting Up MailMate](#)
  - [“Setting Up Outlook 365”](#)
  - [Uninstalling SpamSieve](#)
- Made various internal code modernizations.
- Made the task code more robust.
- Worked around an OS bug that could cause a crash when creating a diagnostic report.
- Fixed a bug where Apple Mail messages trained as good didn’t move to the inbox when the Mac was running in Russian.
- Fixed a bug that could cause a crash when logging errors.
- Updated the Danish and German localizations.

## 2.9.27—December 9, 2016

- Works with Apple Mail under macOS 10.12.2. It’s easiest if you [update](#) to SpamSieve 2.9.27 [before](#) updating to 10.12.2. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve’s filtering accuracy.
- The new **Save Diagnostic Report...** command in the **Help** menu provides an easier way of recording error logs and other information to send to technical support (requires macOS 10.12).
- The [Apple Mail - Remote Training](#) script now lets you specify a different spam mailbox name for each account.
- The [Quit when mail client quits](#) feature now works with Airmail 3.
- The [Outlook - Filter Mailboxes](#) script now filters messages in inboxes with localized names.
- Improved the following sections of the manual:
  - [Requirements](#)
  - [Does SpamSieve launch automatically?](#)
  - [Recommended Mail Hosts](#)
  - [Sending in an Error Report](#)
  - [Sending in Apple Mail Rules](#)
  - [Sending in the SpamSieve Log File](#)
- Made various changes to SpamSieve’s logging to work better with macOS 10.12.
- Improved SpamSieve’s checking of the launch agent’s owner and group.
- Improved the debug logging when training as spam in Apple Mail.
- Fixed a regression where the **Change Settings** command in Apple Mail did not show the current settings using the default button.

- SpamSieve now removes the **Show Tab Bar** menu item and associated functionality on macOS 10.12, since they don't make sense for its user interface.
- Updated to Xcode 8.1.

#### 2.9.26—October 18, 2016

- Works with Apple Mail under macOS 10.12.1. It's easiest if you [update](#) to SpamSieve 2.9.26 [before](#) updating to 10.12.1. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve's filtering accuracy.
- SpamSieve now tells Apple Mail's junk filter when incoming messages are *not* junk (instead of only when they *are* junk). This should help prevent the confusing behavior of Mail displaying good messages in gold/brown text if its filter (or a server filter) disagreed with SpamSieve. Reminder: You can also have SpamSieve override the message text color by enabling `AppleMailAllJunkMessagesUseBlackText` in the [esoteric preferences](#).
- SpamSieve now uses the new `os_log` subsystem on macOS 10.12.
- Adjusted the sizes of the Dock icon status indicators to work around a font change in macOS 10.12.
- The version number of the Apple Mail plug-in is now synchronized with the version number of SpamSieve itself to reduce confusion for those using [Mail Plugin Manager](#).
- Added the [Apple Mail - Mark Server Spam Messages as Read](#) script.
- Improved the following section of the manual:
  - [Recommended Mail Hosts](#)
  - [Requirements](#)
  - [Setting Up an Apple Mail Drone](#)
  - [Setting Up Postbox](#)
  - [What information should I include when I report a problem?](#)
  - [Why is SpamSieve not catching my spam?](#)
- Worked around a badly worded OS certificate error when checking for a software update.
- Adjusted SpamSieve's package resources to work around several code signing issues with macOS 10.12.
- Fixed a bug where Apple Mail could repeatedly report the same error message.
- Fixed a bug where the Portuguese localizer was not given credit in the **About SpamSieve** window.

#### 2.9.25—September 19, 2016

- Works with Apple Mail under macOS 10.12. It's easiest if you [update](#) to SpamSieve 2.9.25 [before](#) updating to 10.12. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve's filtering accuracy.
- Apple Mail
  - Improved the positioning of the SpamSieve items in Apple Mail's **Message** menu.

- If SpamSieve’s plug-in is incompatible with the current version of Apple Mail, the error message now includes a button to join the [SpamSieve public beta](#).
- The [Apple Mail - Server Junk Mailbox](#) script now has an option to mark good messages as read.
- The [Apple Mail - Move if Spam](#), [Apple Mail - SaneBox](#), and [Apple Mail - Server Junk Mailbox](#) scripts now have an option to not change the junk status in Apple Mail, as that can be very slow with some mail servers.
- Removed a workaround that sometimes prevented messages trained in Apple Mail on Mac OS X 10.10 from updating the junk status in Mail.
- SpamSieve is more careful about only modifying its launch agent file when it’s actually changed, so as not to arouse the suspicions of anti-virus software.
- Improved the reporting of Apple Mail training errors.
- Improved the error reporting when Apple Mail is having trouble launching SpamSieve.
- Improved the error message if SpamSieve finds that its launch agent has been unexpectedly deleted.
- Fixed a bug where the Apple Mail plug-in could report an error about not being able to create a file.
- Fixed a bug where the Apple Mail plug-in was missing its Spanish localization.
- Fixed a bug where SpamSieve could get stuck in an auto-launch, auto-quit cycle when logging into a slower Mac.
- Fixed a bug where Apple Mail could hang when processing incoming messages if SpamSieve was showing a modal window, such as the trial expiration alert.
- Microsoft Outlook
  - Worked around an Outlook error getting a message’s subject. To get this fix, choose **Install Outlook Scripts** from the SpamSieve menu.
  - Updated the **Outlook - Move If Spam**, [Outlook - Filter Mailboxes](#), and [Outlook - Remote Training scripts](#) scripts to work around a bug in Outlook 2016 that could make a spam message disappear if Outlook could not find the **Junk E-mail** folder.
  - The [Outlook - Filter Mailboxes](#) script is better at handling errors from Outlook in getting the message’s subject.
  - The [Outlook - Filter Mailboxes](#) script no longer tries to apply an empty category name to good messages.
  - Fixed a bug where the [Outlook - Filter Mailboxes](#) script only filtered one mailbox per account.
  - Worked around an OS issue where the [Outlook - Filter Mailboxes](#) script would report a System Events error.
- Improved the following section of the manual:
  - [Consolidating Spam From Multiple Filters](#)
  - [Correct All Mistakes](#)
  - [Does SpamSieve prevent me from receiving messages?](#)
  - [Exclude my addresses](#)
  - [Filtering Spam During Power Nap](#)
  - [Outlook Customization](#)
  - [Requirements](#)
  - [Sending in an Error Report](#)
  - [Setting Up Airmail](#)
  - [Setting Up an Apple Mail Drone](#)

- [Setting Up Apple Mail](#)
- [Setting Up Gmail, iCloud, Yahoo, AOL, or Other Web Mail](#)
- [Setting Up MailMate](#)
- [Turning Off the Fastmail Spam Filter](#)
- [Turning Off the Gmail Spam Filter](#)
- [Turning Off the Yahoo Mail Spam Filter](#)
- [Using a Spam Mailbox on the Server](#)
- [What can I do if my Spam mailbox in Apple Mail disappeared?](#)
- [What can I do if the corpus file is damaged?](#)
- [What can I do if the statistics database is damaged?](#)
- [Why do good messages keep going to the Junk or Spam mailbox?](#)
- [Why does the “Junk” mailbox appear in Apple Mail?](#)
- Renamed “Mac OS X” to “macOS” throughout the app and documentation.
- Made various code modernizations.
- Updated to Xcode 8.
- The distribution disk image is now signed.
- Updated the Spanish localization.
- [Infinisys](#)<sup>124</sup> customers can now participate in [SpamSieve public betas](#).
- If you try to activate SpamSieve when its Dock icon is hidden, it now reports how you can show the Dock icon.
- Worked around a Postbox issue that could make SpamSieve not realize that it had seen certain messages before.
- If logging a mail client error to Console fails, SpamSieve will now try to report the error via an alert window so it’s not lost.
- Improved the handling and reporting of file handle errors.
- Improved SpamSieve’s reporting of permissions errors when reading files.
- Improved the error reporting and debug logging.
- Fixed a bug identifying the current mail client.
- Fixed a bug that could cause an autorelease pool error when reporting a crash.
- Fixed a bug where SpamSieve would log errors to Console at launch on Mac OS X 10.6.

## 2.9.24—March 1, 2016

- Works with Apple Mail under Mac OS X 10.11.4. It’s easiest if you [update](#) to SpamSieve 2.9.24 [before](#) updating to 10.11.4. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made some optimizations so that SpamSieve launches faster and sorting and deleting in the **Blocklist**, **Whitelist**, and **Corpus** windows is faster.
- The **Train as Good** command in Apple Mail is better at finding which inbox to move the message back to.
- The [Outlook - Filter Mailboxes.app](#) file is now codesigned for Gatekeeper, so it will work without your having to change System Preferences to allow applications downloaded from **Anywhere**.

---

<sup>124</sup><http://www.infinisys.co.jp/product/spamsieve/>

- The [Apple Mail - Move If Spam](#) script can now color or flag messages based on how spammy they are.
- Improved the following sections of the manual:
  - [Automatically Deleting Old Spam Messages](#)
  - [Checking the Airmail Setup](#)
  - [Exclude my addresses](#)
  - [How can I open the Library folder?](#)
  - [Setting Up Airmail](#)
  - [Setting Up Apple Mail](#)
  - [Setting Up MailMate](#)
  - “Setting Up Outlook 365”
  - [Use Growl global notification system](#)
- SpamSieve now uses a different and more reliable strategy to prevent the OS from keeping it stuck in a partially launched state.
- Added an experimental option for Apple Mail to use black text for messages marked as junk but not processed by SpamSieve, overriding the low-contrast color that Mail added in Mac OS X 10.11. For SpamSieve’s black text, [click here](#)<sup>125</sup>; for the default brown text [click here](#)<sup>126</sup>.
- The [Uninstall Apple Mail Plug-In...](#) command now removes the `Launch SpamSieve.scpt` file.
- When running as background applications, the [Apple Mail - Remote Training](#), [Apple Mail - SaneBox](#), and [Apple Mail - Server Junk Mailbox](#) scripts no longer launch Mail if it is not already running.
- Improved the error handling in the [Apple Mail - Discard Spam](#) script so that it can now delete most of the messages even if a few result in errors.
- Reduced SpamSieve’s memory use when type-selecting in the **Corpus**, **Blocklist**, and **Whitelist** windows.
- SpamSieve is better able to function when the system is unable to tell it where the user’s home folder is.
- Improved the error reporting for the [Software Update...](#) command.
- Modernized the **Software Update** code that checks whether your OS version is new enough to run the new version of SpamSieve.
- The SpamSieveHelper application will now quit in the rare event that another copy is already running.
- Made some changes to try to work around a rare bug where SpamSieve’s Apple Mail plug-in didn’t load until after the first few messages had been downloaded from the server, leading to them being filtered directly to the **Spam** mailbox rather than through SpamSieve.
- Worked around an issue where an internal path conversion error from `NSFileManager` could cause SpamSieve to interrupt spam filtering with an error dialog. Now SpamSieve will simply log an “Error looking up image for address” message to the Console and continue filtering.
- Made various code modernizations.
- Made various changes to the build system.

## 2.9.23—December 8, 2015

<sup>125</sup>`x-spamsieve://default?k=AppleMailAllJunkMessagesUseBlackText&v=YES`

<sup>126</sup>`x-spamsieve://default?k=AppleMailAllJunkMessagesUseBlackText&v=NO`

- Works with Apple Mail under Mac OS X 10.11.2. It's easiest if you [update](#) to SpamSieve 2.9.23 [before](#) updating to 10.11.2. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made a variety of changes to work around a bug in Mac OS X 10.11 in which (in rare cases) the system would start to launch SpamSieve but not load any of its code, leaving it stuck in a partially launched state. This would particularly happen if Mail itself was auto-launched by the system after your Mac booted. This could lead to Apple Mail hanging (while waiting for SpamSieve), spam messages left in the inbox (because the Mail plug-in was forced to assume they were good), and high Mail memory use. SpamSieve's launch agent now tries to detect this situation and quit the stuck SpamSieve process, allowing it to relaunch normally. If this is unsuccessful, the Mail plug-in will report an error explaining what is going on and how you can manually fix it.
- The [Apple Mail - Server Junk Mailbox](#) script can now move the spams to per-account spam mailboxes, has better error reporting, and has an option to enable debug logging.
- The [Apple Mail - SaneBox](#) script now has an option to enable debug logging.
- Made some improvements to the statistics database to be more resilient to errors and also report them better.
- SpamSieve is better at handling errors if it gets disconnected from Apple Mail in the middle of processing a message.
- SpamSieve will no longer try to use Apple Mail's **background activity count** scripting property on Mac OS X 10.11 because it's known to be broken. This will reduce unnecessary error logging to Console.
- SpamSieve no longer creates an **App Store Receipts** folder, since it would always be empty.
- Updated code for Xcode 7.1.
- Fixed the size of the distribution disk image window.
- Worked around a Finder bug that could cause the disk image's icons to be misaligned if the `AppleShowAllFiles` option was enabled.

## 2.9.22—October 21, 2015

- Works with Apple Mail under [Mac OS X 10.11.1](#). It's easiest if you [update](#) to SpamSieve 2.9.22 [before](#) updating to 10.11.1. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- If SpamSieve detects that training a message didn't work because of an AppleScript bug in Mac OS X 10.11, it will now direct you to the new [Duplicate Apple Mail Accounts](#) section of the manual for a workaround.
- When filtering incoming messages, Apple Mail will now wait longer for SpamSieve to launch in case the system delayed respawning the launch agent. Thus, spam messages are more likely to be filtered rather than left in the inbox.
- If the launch agent is set to be continuously running, it no longer quits itself when Mail quits or SpamSieve quits/crashes. This should help ensure that Mail is able to relaunch SpamSieve right away, without Mac OS X 10.11 throttling the launch agent.
- The [Apple Mail - Discard Spam](#) script now has an option to set the retry delay to work around a problem with spam messages being left in the trash if Mail failed to delete them.
- Improved the following sections of the manual:

- [Checking the Apple Mail Setup](#)
- [Checking the Outlook 2011 Setup](#)
- [Faster Apple Mail Training](#)
- [Why do good messages move to the wrong inbox when trained in Apple Mail?](#)

## 2.9.21—September 28, 2015

- Works with Apple Mail under Mac OS X 10.11 El Capitan. It’s easiest if you [update to SpamSieve 2.9.21](#) before updating to El Capitan. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve’s filtering accuracy.
- In Apple Mail on Mac OS X 10.11, SpamSieve now overrides the text color in the message list to prevent unreadable brown text on a colored background.
- Microsoft Outlook 2016 removes the **Run AppleScript** rule action feature. This makes it impossible to create a rule that automatically processes incoming messages with SpamSieve. We recommend using the “send-a-smile” button in Outlook’s main window (below the search field) to send Microsoft feedback, asking them to prioritize this feature. Please see [this forum post](#) for more information and workarounds for using SpamSieve with Outlook 2016.
- Added the [Outlook - Filter Mailboxes](#) script as a workaround for automatically filtering messages with Outlook 2016.
- Added support for App Transport Security on Mac OS X 10.11.
- Modernized code for the Xcode 7 compiler and the Mac OS X 10.11 SDK.
- The **About**, **Software Update**, and help windows now use the San Francisco font on Mac OS X 10.11.
- Added the following sections to the manual:
  - [Filtering Spam During Power Nap](#)
  - [Should I download SpamSieve from this free site?](#)
- Improved the following sections of the manual:
  - [Automatically Deleting Old Spam Messages](#)
  - [Checking the Apple Mail Setup](#)
  - [Correct All Mistakes](#)
  - [Installing SpamSieve](#)
  - [iPhone Spam Filtering](#)
  - [Play sound](#)
  - [Save false negatives to disk](#)
  - [Sending in an Error Report](#)
  - [Sending in Apple Mail Rules](#)
  - [Setting Up Airmail](#)
  - [Setting Up an Apple Mail Drone](#)
  - [Setting Up Gmail, iCloud, Yahoo, AOL, or Other Web Mail](#)
  - [“Setting Up Outlook 365”](#)
  - [Spam Message Colors in Apple Mail](#)
  - [SpamSieve and Multiple Macs](#)
  - [Turning Off the Gmail Spam Filter](#)

- [What can I do if Apple Mail is crashing?](#)
- [Why does a message disappear or go back to the spam mailbox after I train it as good?](#)
- When SpamSieve encounters a permissions error, it now reports on any applicable ACLs (Access Control Lists).
- Improved the error message when your version of SpamSieve is too old for the current version of Mac OS X.
- Added “(?)” to error text to help people know what “Help button” refers to.
- If a PDF file attached to an e-mail triggers an OS bug that leads to an infinite loop, SpamSieve now aborts the `spamsieve-reader` process after 30 seconds. Previously, the process (and your fan) would keep running forever and possibly freeze the mail client.
- Worked around a bug in Mac OS X 10.11 that could cause a crash during [Software Update...](#)
- Worked around a bug in Mac OS X 10.6 and 10.7 that could cause a crash.
- Added defensive coding to try to prevent a crash when saving the corpus to disk.
- Fixed a regression that could cause an error when switching applications.
- Fixed a regression where SpamSieve wasn’t able to reset the corpus.
- Fixed a regression where the Entourage scripts could not be installed.
- Fixed a bug where [Software Update...](#) would continue offering updates in the same session in which you had held down the Option key.
- Fixed a bug where SpamSieve could crash when sending data to a helper tool that exited unexpectedly.
- Fixed a bug where a text field in the crash reporter was truncated.
- Fixed a few small memory leaks.
- Updated the German localization.

## 2.9.20—June 3, 2015

### General

- Made various changes to improve SpamSieve’s filtering accuracy.
- Apple’s server-side iCloud spam filter has recently become more aggressive. As a result, many people have been confused by the sudden increase in messages in the **Junk** mailbox (rather than SpamSieve’s **Spam** mailbox). iCloud’s spam filter cannot be turned off, but the [Why does the “Junk” mailbox appear in Apple Mail?](#) section of the manual and the new [Consolidating Spam From Multiple Filters](#) section explain some of the options for dealing with this.
- SpamSieve’s launch agent process no longer runs when Apple Mail is not running, which should reduce overall memory use.
- Dates in the log are now shown in the local time zone.
- **Trained** entries in the log now include the sender’s address.
- The Apple Mail plug-in installer now checks that file ownership is enabled on the volume containing your home folder. This is necessary for proper operation of SpamSieve’s launch agent and, thus, launching and training from Apple Mail.
- When the trial period is over, the alert now has a **Help** button that opens the instructions for uninstalling.
- The [Uninstall Apple Mail Plug-In...](#) command is now available even after the trial period has ended.
- Improved the fonts in the **About** and **Software Update** windows.



- Added accessibility labels in the **Software Update** new **News** windows.
- Added the following sections to the manual:
  - [Checking the Airmail Setup](#)
  - [Consolidating Spam From Multiple Filters](#)
  - [Turning Off the Fastmail Spam Filter](#)
- Improved the following sections of the manual:
  - [Can I delete spam messages that are in the spam folder?](#)
  - [Changing the Name of the Spam Mailbox](#)
  - [Checking the Airmail Setup](#)
  - [Checking the Apple Mail Setup](#)
  - [“Checking the Outlook 365 Setup”](#)
  - [Checking the Postbox Setup](#)
  - [Consolidating Spam From Multiple Filters](#)
  - [Correct All Mistakes](#)
  - [Does SpamSieve launch automatically?](#)
  - [Does SpamSieve stop Web bugs?](#)
  - [Faster Apple Mail Training](#)
  - [How can I copy my training data to another machine?](#)
  - [How should I configure the junk filter on my mail server?](#)
  - [“Setting Up Outlook 365”](#)
  - [Spam Message Colors in Apple Mail](#)
  - [Train SpamSieve whitelist](#)
  - [Turning Off the Gmail Spam Filter](#)
  - [Use Bayesian classifier](#)
  - [Use macOS Contacts](#)
  - [What can I do if Apple Mail is crashing?](#)
  - [What can I do if my Spam mailbox in Apple Mail disappeared?](#)
  - [What can I do if the corpus file is damaged?](#)
  - [Why does SpamSieve always need an update when macOS is updated?](#)
  - [Why does the “Junk” mailbox appear in Apple Mail?](#)
  - [Why is SpamSieve not catching my spam?](#)
- [Reinstalling a Fresh Copy](#) is now its own section of the manual, and SpamSieve will direct you there if it finds that one of its files is missing.

## AppleScript

- The [Apple Mail - SaneBox](#) and [Apple Mail - Server Junk Mailbox](#) scripts:
  - Can now be configured to move any color of spammy messages directly to the trash and to apply flag colors so that you can sort by spamminess.
  - Have an option to move the most spammy messages to trash.
  - Can now be saved as standalone applications to run on a more regular schedule than when run via a Mail rule.
- The [Apple Mail - Remote Training](#) script now has an option to mark the trained spam messages as read.
- The [Apple Mail - SaneBox](#) script now has a configurable mailbox name.
- The [Apple Mail - Discard Spam](#) script is better at handling errors from Mail.
- Added the [Apple Mail - List Mailboxes](#) script.

- The [Copy Whitelist Addresses](#) script can now copy blocklist addresses and now restricts itself to “Is Equal to” rules.
- Fixed an error reporting bug in the [Apple Mail - Discard Spam](#) script.
- Fixed a regression in the [Apple Mail - Remote Training](#) script.
- Fixed an error reporting bug in the [Apple Mail - SaneBox](#) script.

### Error Handling

- SpamSieve will now recreate the log file’s folder if it unexpectedly disappears after the application has launched, perhaps due to CleanApp. If this affects you, SpamSieve will make a note in the Console log.
- Improved SpamSieve’s error handling and recovery when there is an error creating or updating the log file.
- The [Uninstall Apple Mail Plug-In...](#) command will now retry if there’s an error communicating with Mail and report a better error if it still doesn’t succeed.
- When training from Apple Mail, SpamSieve will now report a better error if it detects that the necessary SpamSieveHelper application is not running.
- If SpamSieve detects that one of its files is missing, i.e. that the application is damaged, it now presents a better error message.
- When there is an error reading the corpus or history database, the error alert now has a clickable Help button instead of inline URL text.
- The Entourage scripts can now log errors to Console.
- SpamSieve will now log an error if it’s not installed in the **Applications** folder, as this can prevent proper functioning with Airmail (due to sandbox restrictions).
- Improved the error message if Apple Mail can’t launch SpamSieve.
- Errors for corrupt files now link to the relevant Web pages that explain how to fix them.
- Improved the error message when you’re using a version of SpamSieve that’s too old for your version of Apple Mail.
- Improved error reporting when a temporary folder cannot be created.
- Improved the error message for incorrect serial numbers.
- SpamSieve now reports permissions information if there’s an error opening the statistics database.

### Bug Fixes

- Worked around a bug where Microsoft Outlook does not always correctly return a message’s source. This could lead to spam messages being classified as good because SpamSieve had no information to work from. To get this fix, choose **Install Outlook Scripts** from the **SpamSieve** menu.
- Worked around a text conversion bug in Mac OS X 10.10.3.
- SpamSieve will no longer repeatedly try to fix a file’s owner if ownership is ignored on the volume.
- Fixed a bug where SpamSieve could report an internal error if it received an Apple event while in the process of quitting.
- Fixed a bug that could cause an internal error writing to SpamSieve’s log file when the application was quitting.
- Fixed a regression where the Outlook 14 installer didn’t properly migrate installed script files.
- Fixed a bug abbreviating long rules in the log.
- Date formatters now use the POSIX local where appropriate.

**2.9.19—January 27, 2015**

- Works with Apple Mail under Mac OS X 10.10.2. It's easiest if you [update to SpamSieve 2.9.19](#) before updating to Mac OS X 10.10.2. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- To make future OS updates smoother:
  - You can wait to update Mac OS X until a new version of SpamSieve has been released. The latest compatibility information is always available at the top of the [SpamSieve Support](#) page. To prevent Mac OS X from updating itself without asking you, go to the **App Store** section of **System Preferences** and make sure that **Install OS X updates** is unchecked.
  - You can sign up to receive the [public beta versions](#) of SpamSieve. Then you will likely already have a compatible version of SpamSieve installed when the OS update first becomes available.
- Added the [Uninstall Apple Mail Plug-In...](#) command in [the SpamSieve menu](#).
- SpamSieve is now more aggressive about auto-training whitelist rules to prevent false positives.
- SpamSieve is now 33% faster at reading the corpus and 48% faster at writing it. This improves the launch time and overall application responsiveness.
- The Apple Mail **Train as Good** command is better at determining when a message is inside of a junk mailbox with a localized name.
- The [Apple Mail - Remote Training](#) script no longer times out when there are lots of messages in the training mailbox. It also has new options for changing the name of the spam mailbox and for enabling debug logging.
- The [Apple Mail - SaneBox](#) and [Apple Mail - Server Junk Mailbox](#) scripts now set the junk status and color for spam messages.
- Added the following sections to the manual:
  - [Checking the GyazMail Setup](#)
  - [Separate Spam Folders for Each Account \(Outlook 2011\)](#)
  - [What can I do if the corpus file is damaged?](#)
  - [What can I do if the statistics database is damaged?](#)
- Improved the following sections of the manual:
  - [iPhone Spam Filtering](#)
  - [Installing SpamSieve](#)
  - ["Setting Up Outlook 365"](#)
  - [Updating From a Previous Version](#)
- Added improved [instructions](#) for installing and running supplemental AppleScripts.
- If Outlook reports an error when creating the **Uncertain Junk** category, SpamSieve now explains how you can create it manually.
- SpamSieve can now log the contents of the **LaunchAgents** folder if there is a problem.
- When the SpamSieve application is damaged and needs to be reinstalled, it now links to some more extensive online instructions for doing so.
- Improved the error reporting when SpamSieve's log file can't be written to.
- If there's an error removing the old copy of the Apple Mail plug-in and fixing the file permissions/ownership doesn't help, SpamSieve now instructs you how to remove the file manually.
- Improved the text in the **Welcome** window. Also, the window is now shown later in the launch process so that the referenced **Help** menu is available.

- The [About SpamSieve](#) window now uses the new system font on Mac OS X 10.10.
- The [About SpamSieve](#) window now uses the system language names when crediting localizers, to reduce the number of strings that localizers need to keep up-to-date.
- Increased the font size in the [Software Update...](#) window on Mac OS X 10.10.
- Added the `ShowResetAlert` user default to show the corpus/history reset window if the user can't hold down the proper modifier keys.
- Added `QuitMailWhenMacSleeps` to the [esoteric preferences](#). This quits Mail when the Mac sleeps and relaunches it when the Mac wakes. This works around an OS bug that can cause messages not to be moved to the **Spam** mailbox if Mail received them right after the Mac woke from sleep.
- Worked around a string encoding bug in Mac OS X 10.10.
- Fixed a bug where the Apple Mail plug-in would cause unnecessary messages about `LSUIElement` and the sandbox to be logged to Console.
- Fixed a bug where a change in system font metrics caused some text in the **Preferences** and **Statistics** windows to be truncated.
- Fixed spurious log messages from SpamSieveHelper when running on Mac OS X 10.10.
- Added defensive check to prevent trying to fix the ownership of certain folders.
- Fixed a bug where toolbar buttons in the rules and corpus windows were always enabled when running on Mac OS X 10.10.
- Worked around an OS bug that prevented bookmark files from being resolved.
- Worked around an OS bug that could cause SpamSieve's log file to be created in the wrong location.
- Updated the German and Spanish localizations.

## 2.9.18—November 17, 2014

- Works with Apple Mail under Mac OS X 10.10.1. It's easiest if you [update to SpamSieve 2.9.18](#) before updating to Mac OS X 10.10.1. (To prevent Mac OS X from updating itself without asking you, go to the **App Store** section of **System Preferences** and make sure that **Install OS X updates** is unchecked.) In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from the [SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Added preliminary support for [Microsoft Outlook 15.3](#)<sup>127</sup> (part of Office 365). This is described in the "Setting Up Outlook 365" section of the manual.
- Added the following sections to the manual:
  - "Setting Up Outlook 365"
  - "Checking the Outlook 365 Setup"
  - [What can I do if Apple Mail is crashing?](#)
- Improved the following sections of the manual (among others):
  - [Setting Up Airmail](#)
  - [Setting Up GyazMail](#)
  - [Setting Up MailMate](#)
  - [Why does SpamSieve always need an update when macOS is updated?](#)
- The [Apple Mail - Discard Spam script](#) is faster and more reliable for large mailboxes.

---

<sup>127</sup><http://blogs.office.com/2014/10/31/new-outlook-mac-available-office-365-customers/>

- Improved the error reporting when writing to the log file and the disk is full.
- SpamSieve is better able to recover from incorrect launch agent file ownership.
- The [Quit when mail client quits](#) feature now works with Airmail 2.
- The **Blocklist** and **Whitelist** windows now display the number of rules using commas if there are more than 1,000.
- The [Purchase...](#) window now accepts serial numbers copied and pasted from a PDF of an order confirmation, after the browser has transliterated the dashes.
- Updated the toolbar icons for Mac OS X 10.10.
- Updated the disk image icon for Mac OS X 10.10.
- Worked around a bug in Mac OS X 10.10 that could cause SpamSieve to freeze at launch.
- Worked around a string encoding conversion bug in Mac OS X 10.10.
- The crash reporter now reports more information if it couldn't find any matching crash log files.

## 2.9.17—October 16, 2014

- Works with Apple Mail under [Mac OS X 10.10 Yosemite](#). It's easiest if you [update to SpamSieve 2.9.17](#) before updating to Mac OS X 10.10. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Added the following sections to the manual:
  - [Does SpamSieve stop Web bugs?](#)
  - [Why do good messages move to the wrong inbox when trained in Apple Mail?](#)
  - [Why does a message disappear or go back to the spam mailbox after I train it as good?](#)
  - [Does SpamSieve prevent me from receiving messages?](#)
  - [Can other Apple Mail plug-ins cause problems with SpamSieve?](#)
- Improved the following sections of the manual (among others):
  - [Correct All Mistakes](#)
  - [How should I configure the junk filter on my mail server?](#)
  - [iPhone Spam Filtering](#)
  - [Show Whitelist](#)
  - [Updating From a Previous Version](#)
- Updating OS versions is smoother since SpamSieve is better at finding disabled copies of its Apple Mail plug-in.
- Worked around a change in Mac OS X that could cause the [Quit when mail client quits](#) feature to not work when running in Japanese.
- Improved the crash reporter's error reporting.
- Improved debug logging for the Apple Mail training scripts.
- Fixed a bug where SpamSieve could crash if there was an error writing to its log file.
- Fixed a bug where SpamSieve would, in rare cases, try to change the ownership of a temporary folder unnecessarily.
- We need help keeping SpamSieve's Japanese localization up-to-date. Please contact [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>128</sup> if you're interested.

---

<sup>128</sup><mailto:spamsieve@c-command.com>

## 2.9.16—September 17, 2014

- Works with Apple Mail under [Mac OS X 10.9.5](#)<sup>129</sup>. It's easiest if you [update to SpamSieve 2.9.16](#) before updating to Mac OS X 10.9.5. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose [Install Apple Mail Plug-In](#) from [the SpamSieve menu](#). Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Improved compatibility with pre-release versions of Mac OS X 10.10 Yosemite.
- Made various changes to improve SpamSieve's filtering accuracy.
- Updated the Outlook and Entourage scripts for compatibility with the upcoming Mac OS X 10.0. If you're using one of those mail clients, you should update the scripts by choosing [Install Outlook Scripts](#) or [Install Entourage Scripts](#) from [the SpamSieve menu](#).
- Updated the [Apple Mail - Discard Spam](#), [Apple Mail - Move If Spam](#), [Apple Mail - Remote Training](#), [Apple Mail - Save Spam](#), and [PowerMail - Uncertain Spam Condition](#) scripts to work around a bug in the upcoming Mac OS X 10.10. If you are using these scripts, you will need to download and install fresh copies of them.
- Updated the [Apple Mail - Remote Training](#), [Apple Mail - SaneBox](#), and [Apple Mail - Server Junk Mailbox](#) scripts to work around a problem with duplicate messages created from deleted messages that Mail had not expunged. If you are using these scripts, you will need to download and install fresh copies of them.
- Added a new method of hiding SpamSieve's Dock icon that doesn't require editing the `Info.plist` file. For more information, see the [How can I hide SpamSieve's Dock icon?](#) section of the manual.
- Added the [Faster Apple Mail Training](#), [Why don't I see the SpamSieve commands in Apple Mail's Message menu?](#), and [Recommended Apple Mail Customizations \(macOS 10.8 and Earlier\)](#) sections of the manual.
- Improved the [Automatically Deleting Old Spam Messages](#), [Changing the Name of the Spam Mailbox](#) sections, [Show Blocklist](#), [Show Whitelist](#), [Requirements](#), [Correct All Mistakes](#), [Separate Spam Mailboxes for Each Account](#), [Use macOS Contacts](#), [Redirecting Good Messages to Another Account](#), [Apple Mail Customization](#), [How should I configure the junk filter on my mail server?](#), [Updating From a Previous Version](#), and [Uninstalling SpamSieve](#) sections of the manual.
- SpamSieve is better at repairing folder ownership and permissions.
- SpamSieve is better able to recover from errors when creating temporary folders.
- Made lots of code modernizations.
- By default, training a message as good in Apple Mail no longer clears its colored flags. This can be adjusted using the `AppleMailTrainGoodClearFlags` option in the [esoteric preferences](#).
- [Esoteric preferences](#) links are now directly clickable in the Apple Help and PDF manual.
- Worked around a problem where Apple Mail could hang at launch if MailTags was installed.
- Removed spurious warnings about extra Apple Mail preferences files.
- Improved error reporting when SpamSieve can't connect to the update server.
- Removed the Option-key workaround to have SpamSieve try to update the Apple Mail plug-in's `Info.plist` file (based on installed version of Mail) because it's no longer effective.
- Fixed a bug reporting an error from running a compiled AppleScript.
- Improved the crash reporter.
- Fixed a crash when reporting file errors.

---

<sup>129</sup><http://support.apple.com/kb/HT6400>

- We need help keeping SpamSieve’s Japanese localization up-to-date. Please contact [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>130</sup> if you’re interested.

## 2.9.15—June 30, 2014

- Works with Apple Mail under [Mac OS X 10.9.4](#)<sup>131</sup>. It’s easiest if you update to SpamSieve 2.9.15 before updating to Mac OS X 10.9.4. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose **Install Apple Mail Plug-In** from the **SpamSieve** menu. Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Improved compatibility with pre-release versions of Mac OS X 10.10 Yosemite.
- Made various changes to improve SpamSieve’s filtering accuracy.
- SpamSieve now requires Mac OS X 10.6.8 or later. Versions of SpamSieve for [Mac OS X 10.5 and earlier](#) are available.
- Modernized lots of code and removed old code that’s no longer needed for compatibility with legacy OS versions.
- Made changes so that SpamSieve launches faster, especially when `cfprefsd` is slow to respond.
- Added the [Why are messages marked as spam in Apple Mail but not moved?](#) section to the manual.
- Fixed a bug that could cause the [Install Outlook Scripts](#) command to fail if [Parallels Desktop](#)<sup>132</sup> was installed and its stub application for the Windows version of Outlook was enabled.
- The [Apple Mail - SaneBox](#) script now reports errors to Console (since Mail was suppressing them) and no longer times out for very large mailboxes.
- The [Software Update...](#) feature is better at explaining what you can do if installation fails.
- Adjusted the way the [Purchase...](#) window displays the remaining demo time to try to make it clearer.
- Improved the reporting of file permissions errors and damaged sound files.
- Improved the handling of localized strings when the application is damaged.
- Fixed a bug where the release notes in the [Software Update...](#) window were shown in the wrong font.
- Fixed a bug where SpamSieve would auto-train even if you had unchecked all of the filters.
- Updated the Dutch, Japanese, and Spanish localizations.
- We need help keeping SpamSieve’s Japanese localization up-to-date. Please contact [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>133</sup> if you’re interested.

## 2.9.14—May 15, 2014

- Works with Apple Mail under [Mac OS X 10.9.3](#)<sup>134</sup>. It’s easiest if you update to SpamSieve 2.9.14 before updating to Mac OS X 10.9.3. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose **Install Apple Mail Plug-In** from the **SpamSieve** menu. Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve’s filtering accuracy.

---

<sup>130</sup><mailto:spamsieve@c-command.com>

<sup>131</sup><http://support.apple.com/kb/HT6281>

<sup>132</sup><http://www.parallels.com/products/desktop/>

<sup>133</sup><mailto:spamsieve@c-command.com>

<sup>134</sup><http://support.apple.com/kb/HT6228>



- Added the [Does SpamSieve protect me from viruses?](#) and [Why does SpamSieve always need an update when macOS is updated?](#) sections to the manual.
- Improved the [Spam Message Colors in Apple Mail](#), [Correct All Mistakes](#), [Sending in the SpamSieve Log File](#), [Using a Spam Mailbox on the Server](#), [Why does the “Junk” mailbox appear in Apple Mail?](#), and [Checking the Mailsmith Setup](#) sections of the manual, as well as various instructional alerts and error messages.
- The [Import Addresses...](#) command no longer has a file size limit.
- SpamSieve no longer prompts to access the system contacts database if you have [Use macOS Contacts](#) unchecked.
- Made some changes to make SpamSieve launch faster, especially when `cfprefsd` is slow to respond.
- Rewrote the [Apple Mail - Discard Spam](#) script to not rely on GUI scripting and to avoid deleting messages that were already in the trash.
- The [Setting Up Postbox](#) command works better with pre-release versions of Postbox.
- SpamSieve now checks the permissions on more of Apple Mail’s folders.
- If an error occurs during [Install Outlook Scripts](#), SpamSieve will now try to determine whether this was because Microsoft Outlook was not installed properly.
- If your copy of Apple Mail is damaged, SpamSieve will now report this, but it will still let you install the plug-in.
- The training commands in Apple Mail work better with localized mailbox names.
- Added more logging for the Outlook **Train as Good** command.
- The images in the PDF manual and Apple Help are now Retina-resolution.
- Adjusted the font sizes in the PDF manual.

#### 2.9.13—February 25, 2014

- Works with Apple Mail under Mac OS X 10.9.2. It’s easiest if you update to SpamSieve 2.9.13 before updating to Mac OS X 10.9.2. In any case, if you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose **Install Apple Mail Plug-In** from the **SpamSieve** menu. Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#) without consulting SpamSieve.
- Made various changes to improve SpamSieve’s filtering accuracy.
- On Mac OS X 10.9 Mavericks, Apple Mail is slower at moving messages to the **Spam** mailbox when you choose **SpamSieve - Train as Spam** and the inbox when you choose **SpamSieve - Train as Good**. This version of SpamSieve includes some changes to speed this up. It also includes workarounds to move messages faster by using GUI scripting instead of regular AppleScript. To enable the workarounds, please see the `AppleMailTrainSpamGUIScripting` and `AppleMailTrainGoodGUIScripting` options in the [Esoteric Preferences](#) section of the manual.
- Documented the `AppleMailPlugInSetIsJunk` esoteric preference, as it can be used to speed up filtering on Mac OS X 10.9.
- Improved the [Setting Up Airmail](#) section of the manual to recommend not deleting messages from the **Spam** mailbox when using Airmail 1.3.1 (223).
- Added the [Why does the “Junk” mailbox appear in Apple Mail?](#) section to the manual.
- Improved the [Setting Up a MailMate Drone](#) and [iPhone Spam Filtering](#) sections of the manual.
- The `AppleMailTrainSpamGUIScripting` esoteric preference now works if you’ve selected the trash as your mailbox for trained spam messages.



- Optimized and fixed a possible Apple Mail crash when using the [Setting Up an Apple Mail Drone](#) configuration.
- SpamSieve is now able to log more diagnostic information to help track down problems with Apple Mail.
- When a Mac OS X update disables SpamSieve's Apple Mail plug-in, and your Mac is running in a language other than English, SpamSieve is better able to detect this and auto-reinstall the plug-in.
- SpamSieve now cleans up empty folders of disabled Apple Mail bundles.
- When training messages from Microsoft Outlook, SpamSieve now logs errors to the Console. You can also enable extended error logging via the `OutlookScriptDebug` default.

### 2.9.12—December 16, 2013

- Works with Apple Mail under Mac OS X 10.9.1. It's easiest if you update to SpamSieve 2.9.12 before updating to Mac OS X 10.9.1. In any case, if you don't see the SpamSieve commands in Apple Mail's **Message** menu, be sure to choose **Install Apple Mail Plug-In** from the **SpamSieve** menu. Otherwise, with the SpamSieve plug-in not installed, Mail will [move good messages to the spam mailbox](#).
- On Mac OS X 10.9 Mavericks, Apple Mail is slower at moving messages to the **Spam** mailbox when you choose **SpamSieve - Train as Spam**. SpamSieve includes a workaround to move messages faster by using GUI scripting instead of regular AppleScript. To enable the workaround, please see the `AppleMailTrainSpamGUIScripting` option in the [Esoteric Preferences](#) section of the manual.
- Versions 1.2.1 and later of the [Airmail](#)<sup>135</sup> e-mail client include support for SpamSieve. The [Setting Up Airmail](#) section of the manual describes how to use SpamSieve with Airmail.
- It is now possible to set up a [spam filtering drone](#) using the [MailMate](#)<sup>136</sup> e-mail client. This is described in the [Setting Up a MailMate Drone](#) section of the manual.
- The [Flash PowerMate](#) feature is now compatible with (and requires) version 3.0 of the Griffin [PowerMate](#)<sup>137</sup> software.
- You can now hold down the Option key when you click **Check Now** in the [Software Update...](#) window to always download the latest version, even if your version is already up-to-date. This is an easy way to download and re-install a fresh copy of SpamSieve if yours is damaged.
- Added the `AppleMailTrainGoodClearFlags` [esoteric preference](#), for people who use colored flags on their spam messages for purposes other than [indicating the spam level](#).
- If Microsoft Outlook is not able to retrieve a message's source, SpamSieve will now log the message's subject to Console.
- Worked around an OS bug that could cause a crash when SpamSieve was processing certain types of multi-part e-mail messages.
- Improved various error messages.
- Tried to work around a crash by disabling JavaScript in the release notes view.

### 2.9.11—November 7, 2013

- Works with the [Mail Update for Mavericks 1.0](#)<sup>138</sup>.

<sup>135</sup><http://airmailapp.com>

<sup>136</sup><http://freron.com>

<sup>137</sup><http://store.griffintechnology.com/powermate>

<sup>138</sup>[http://support.apple.com/kb/HT6030?viewlocale=en\\_US&locale=en\\_US](http://support.apple.com/kb/HT6030?viewlocale=en_US&locale=en_US)

- Added a workaround for some rare cases where SpamSieve’s commands were not showing in Apple Mail’s **Message** menu.
- Updated the [Apple Mail - Discard Spam](#) script.
- Added some defensive coding to protect against a bug in `_NSDispatchData` that could cause a crash on Mavericks.
- Made various updates and improvements to the manual.

#### 2.9.10—October 22, 2013

- SpamSieve is now compatible with the updated GM build of Mac OS X 10.9 Mavericks. It is recommended that you update to SpamSieve 2.9.10 before installing Mavericks. If you’ve updated to Mavericks first, and you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose **Install Apple Mail Plug-In** from the **SpamSieve** menu.
- The [How can I hide SpamSieve’s Dock icon?](#) section of the manual has been updated for Mac OS X 10.9 Mavericks.
- Improved various other parts of the manual and Read Me.
- Tried to work around a problem where the Outlook installer received an error from the system when the Mac was running in French.

#### 2.9.9—October 7, 2013

- SpamSieve is now compatible with the GM build of Mac OS X 10.9 Mavericks. It is recommended that you update to SpamSieve 2.9.9 before installing Mavericks. If you’ve updated to Mavericks first, and you don’t see the SpamSieve commands in Apple Mail’s **Message** menu, be sure to choose **Install Apple Mail Plug-In** from the **SpamSieve** menu.
- Made various changes to improve SpamSieve’s filtering accuracy.
- Microsoft Outlook 2011’s notification sounds are now available in SpamSieve’s [Notification](#) preferences.
- Added the [Apple Mail - Server Junk Mailbox](#) script. When it’s not possible to [turn off](#) a server-side junk filter (e.g. iCloud’s), this lets SpamSieve save you from mistakes that the server junk filter made by moving any messages that SpamSieve thinks are good back to the inbox. It will also consolidate the spam messages from all the accounts into a single spam mailbox (the same one where SpamSieve is already putting your spam).
- Can now repair the ownership and permissions of the SpamSieve and Apple Mail preferences files if needed. This fixes problems where SpamSieve would lose its registration information or Apple Mail wouldn’t show the SpamSieve menu commands.
- Fixed some problems where the **Open Window** command in Apple Mail was not available or did not always open the specified window.

#### 2.9.8—September 12, 2013

- SpamSieve is now compatible with Mac OS X 10.8.5.
- Made various changes to improve SpamSieve’s filtering accuracy.
- The **Train as Good** command in Apple Mail now considers the message’s CC recipients when determining the proper account inbox.
- The installer is better at working around incorrect Apple Mail folder permissions.
- Improved the [Why is SpamSieve not catching my spam?](#), [Open Log](#), [Setting Up Outlook 2011](#), [SpamSieve and Multiple Macs](#), and various other sections of the manual.
- The AppleScript for [Setting Up a Spam Filtering Drone](#) runs faster now.

- Automatic software updates no longer fail if [Hazel](#)<sup>139</sup> is set to move files in the **Downloads** folder.
- The **Help** menu now includes direct links to important sections of the manual.
- Removed unused code from the Apple Mail plug-in.

### 2.9.7—May 1, 2013

- Improved compatibility with pre-release versions of Mac OS X.
- Made various changes to improve SpamSieve’s filtering accuracy.
- SpamSieve no longer links against AppleScriptKit. This removes some GUI scripting functionality (which is now largely available by other means) but works around an OS bug that could prevent SpamSieve from launching.
- Worked around a bug in Apple Mail’s iCloud rule syncing.
- SpamSieve is better at moving trained messages when Outlook has lost track of the special **Junk E-mail** folder.
- Fixed a problem where Apple Mail couldn’t communicate with SpamSieve when the file permissions were incorrect.
- Fixed a bug where SpamSieve couldn’t load any addresses from Outlook if it reported an error while getting the e-mail address of a contact.
- Fixed a bug editing counts in the **Corpus** window (due to suspected 64-bit OS bug).
- Added more checks that the folders SpamSieve relies upon have the proper permissions.
- Improved error reporting for Apple Mail, Growl, and more.
- Improved handling of file permissions errors.
- The Apple Mail drone script now sets the junk status.
- Wrote a [script](#) that allows SpamSieve to filter messages (in Apple Mail) that have been organized by SaneBox.
- Improved the Japanese localization.
- SpamSieve now requires Mac OS X 10.5 or later.

### 2.9.6—December 19, 2012

- Worked around a [bug](#)<sup>140</sup> in Mac OS X 10.8.2 that could cause spam operations in [Postbox](#)<sup>141</sup> to be very slow. If you’re using Postbox, you can update your SpamSieve plug-in by following steps 1 through 6 in the [Setting Up Postbox](#) section of the manual.
- Made various changes to improve SpamSieve’s filtering accuracy.
- SpamSieve now understands that [@icloud.com](#), [@me.com](#), and [@mac.com](#) are equivalent, so it’s better at finding the proper inbox in Apple Mail when you train a message as good. (For non-Apple IMAP and POP mail accounts, you can define aliases manually, as before. Go to the **Accounts** tab of Mail’s preferences and enter all the addresses—separated by commas—in the **Email Address** field.)
- Customers have reported that Sync Services does not work reliably on Mac OS X 10.8 Mountain Lion. Thus, rather than having Outlook use Sync Services to sync its contacts with the system address book, SpamSieve now offers a feature to load the Outlook address book directly. (This ensures that SpamSieve doesn’t mark messages from people in your address book as spam.) Outlook users are encouraged to make sure that [Use Entourage/Outlook address book](#) is checked in SpamSieve’s preferences and to click the **Load** button. For more information, see the [Use Entourage/Outlook address book](#) section of the manual.

---

<sup>139</sup><http://www.noodlesoft.com/hazel.php>

<sup>140</sup><http://www.openradar.me/12424662>

<sup>141</sup><http://www.postbox-inc.com>

- SpamSieve is now better able to handle invalid data received from a mail program.
- When [Using a Spam Mailbox on the Server](#), SpamSieve is better at handling errors from Mail that could cause a trained spam message to go to the local spam mailbox instead.
- Training a message as good in Apple Mail now removes any flags, in case you were using [Spam Message Colors in Apple Mail](#).
- Added [How should I configure the junk filter on my mail server?](#) to the FAQ.
- The [Automatically Deleting Old Spam Messages](#) section of the manual now includes instructions for Outlook.
- Worked around various file permissions problems that could prevent training in Apple Mail from working.
- Worked around a bug in Migration Assistant that could prevent SpamSieve from working properly with Apple Mail.
- The plug-in and scripts installers are better able to handle non-standard folder structures.
- Fixed a bug where SpamSieve was unable to see the contents of certain malformed messages, leading to poor filtering accuracy.
- Fixed a bug where sometimes setting the date in the **Statistics** window didn't work when SpamSieve was running in 64-bit mode.
- Fixed a regression where where messages trained as good in Apple Mail didn't move back to the inbox if you were using a local spam mailbox and no inbox matched the message's recipients.
- Made various improvements to the manual.

#### 2.9.5—September 21, 2012

- Updated the Apple Mail plug-in to work with [Security Update 2012-004 \(Snow Leopard\)](#)<sup>142</sup> for Mac OS X 10.6.8. If, after installing this update, you don't see the SpamSieve commands in Mail's **Message** menu, it may be necessary to go to the **SpamSieve** menu and choose **Install Apple Mail Plug-In**.
- The AppleScripts for controlling the [Griffin PowerMate](#)<sup>143</sup> seem to trigger a crashing bug in OS X 10.8 Mountain Lion. Thus, SpamSieve's [Flash PowerMate](#) option has been turned off. You can try re-enabling it in the preferences if desired.
- When training a message as good from Apple Mail, SpamSieve is better at figuring out which account it came from.
- Worked around problems on some Macs that could prevent SpamSieve from receiving training commands from Apple Mail on OS X 10.8 Mountain Lion.
- [Import Blocklist Regex Rules](#) is a sample AppleScript that shows how to create blocklist rules using the contents of a text file.
- Made various improvements to the manual.

#### 2.9.4—September 4, 2012

- Made various changes to improve SpamSieve's filtering accuracy.
- Revised and expanded the [Frequently Asked Questions \(FAQ\)](#) to make it easier for people to find, fix, and report problems.
- Fixed a problem where SpamSieve could crash when processing messages from Apple Mail on OS X 10.8, particularly after the Mac had awakened from sleep.

<sup>142</sup><http://support.apple.com/kb/DL1586>

<sup>143</sup><http://www.griffintechology.com/support/powermate>

- Worked around an issue on OS X 10.8 that could cause training SpamSieve from Apple Mail to be very slow.
- The **Train as Good** command in Outlook will now move messages from the trash back to the inbox.
- Made various updates to the manual for OS X 10.8 Mountain Lion, for example clarifying that SpamSieve works (via Apple Mail) during a [Power Nap](#)<sup>144</sup>.
- Worked around a problem where Apple Mail couldn't communicate with SpamSieve if the `/etc/hosts` file was damaged.
- Improved the error reporting when SpamSieve detects that one of its files is damaged.
- Added defensive coding to try to track down a notification icon problem when running in French.
- You can now set the `MJTSoundLoadFromApps` default to false if you want to prevent SpamSieve from looking for notification sounds installed by other applications, e.g. to prevent mounting an encrypted **Microsoft User Data** folder.
- Fixed a bug handling errors if a software update failed; if it succeeded, the `.dmg` file is now deleted to reduce clutter.
- After purchasing, SpamSieve used to show your user image to indicate that it had been successfully personalized. It now shows a generic checkmark to avoid prompting you for Contacts access on OS X 10.8.
- Added an icon for the crash reporter, since it's now displayed under OS X 10.8.
- Fixed a bug where Apple Mail on Mac OS X 10.5 would log (harmless) errors about `_NSAutoreleaseNoPool`.
- Fixed a bug where the Apple Mail plug-in sometimes logged confusing error messages about not being able to launch SpamSieve even though it was already launched.
- Fixed a bug where the Apple Mail plug-in reported the wrong installation path in an error message when running on OS X 10.8.

### 2.9.3—July 19, 2012

- Added support for the forthcoming Mac OS X 10.7.5.
- Fixed a bug that could prevent SpamSieve from auto-launching on the forthcoming OS X 10.8.
- SpamSieve is now able to recover from certain unexpected system errors on OS X 10.8.
- Fixed a layout bug in the German-localized **Statistics** window.
- Improved the [Automatically Deleting Old Spam Messages](#) instructions.
- SpamSieve now tells the system that it can use the integrated GPU, which should reduce battery use on newer MacBook Pros.
- SpamSieve's disk image background is now displayed at Retina quality on eligible Macs running Mac OS X 10.7 or 10.8. (On Mac OS X 10.6, due to an OS bug, it will incorrectly display at double size.)
- Fixed a regression where SpamSieve's disk image icon didn't display properly.

### 2.9.2—July 5, 2012

- Improved compatibility with the forthcoming OS X 10.8 Mountain Lion.
- The recommended condition for the Apple Mail rule is now **Every Message** rather than **Message Type Is Mail**. SpamSieve will auto-update your rules at launch on Mac OS X 10.7 if Mail is running.

---

<sup>144</sup><http://support.apple.com/kb/HT5394>

- SpamSieve is better at detecting a certain type of tricky spam message.
- Worked around an OS bug that prevented SpamSieve from properly analyzing some message attachments.
- False negative files now have the `.eml` extension so that they work with Quick Look, etc.
- The [Setting Up a Spam Filtering Drone](#) section of the manual has been updated with simpler instructions for Apple Mail and new instructions for setting up a drone using Microsoft Outlook 2011.
- Added the [Using a Spam Mailbox on the Server](#) section of the manual (for Apple Mail).
- Updated various graphics for retina displays.
- If the Apple Mail plug-in cannot be installed due to a folder ownership problem, SpamSieve will now ask for an administrator password to try to fix the folder for you.
- Reverted to version 1.2.3 of the Growl SDK to avoid problems with high CPU usage, internal errors, and crashes.
- Improved SpamSieve’s reporting of unexpected errors as well as script errors from Apple Mail.
- SpamSieve no longer responds at all to certain invalid commands. This should work around an OS bug that could lead to crashes.
- The crash reporter can now make recommendations for you based on the contents of the crash log.
- Added a link to the forum in the **Help** menu.

### 2.9.1—April 26, 2012

- Added support for Microsoft Outlook 2011 SP2 (a.k.a. 14.2.x). If SpamSieve can detect that you were using Outlook 2011 before, and that SP2 has been installed, SpamSieve will auto-update its scripts automatically. Otherwise, you can choose [Install Outlook Scripts](#) from the **SpamSieve** menu. Either way, the SpamSieve rules in Outlook will continue to work without modification.
- SpamSieve now tries to detect whether its Apple Mail plug-in is damaged and auto-heal the installed copy if necessary.
- If there’s an error updating SpamSieve’s Apple Mail plug-in, it now reports more information to try to diagnose the problem.
- If the Apple Mail plug-in detects that it’s damaged, it will alert the user to download and install a fresh copy.
- SpamSieve now checksums the Outlook script files (both the installed and built-in copies) to detect whether they are damaged.
- Made a change to eliminate a particular cause of false positives for some users.
- SpamSieve no longer triggers Mac OS X’s “accept incoming network connections” firewall dialog.
- Added some exception guards to work around bugs in the Growl SDK.
- When an unexpected error occurs and no stack trace is available, SpamSieve will now try to report the approximate location.
- Improved the [What information should I include when I report a problem?](#) section of the manual.

### 2.9—April 3, 2012

- Added support for upcoming versions of Mac OS X.
- Made various changes to improve SpamSieve’s filtering accuracy.

- SpamSieve is now code-signed using a [Developer ID certificate](#)<sup>145</sup> for Gatekeeper.
- When training an Exchange message as good in Apple Mail, SpamSieve is better at moving it to the proper inbox.
- Processing incoming messages with Outlook is more efficient. To take advantage of this change, choose **Install Outlook Scripts** from the **SpamSieve** menu.
- If you’ve used the **SpamSieve - Change Settings** command in Apple Mail to tell SpamSieve not to use a local spam mailbox, training a message as spam will now try to move the message to a spam mailbox on the same server account, rather than always using the first account.
- Added support for training messages as spam via [Herald](#)<sup>146</sup> (version 2.1.2 and later), a notification plug-in for Apple Mail.
- When [sorting spam messages by color in Apple Mail](#), you can now use **Grey** as a synonym for **Gray**.
- The **score** script command has a new **auto training** parameter that can be used to override [the setting](#) in the preferences on a case-by-case basis. This might be useful, for example, if you’re writing an AppleScript to triage messages that have already been classified, and you just want to get SpamSieve’s opinion without having to make any corrections.
- Adjusted the [drone AppleScripts](#) so that they’re easier to troubleshoot.
- If Apple Mail gives SpamSieve empty data for a message, the plug-in now assumes the message is good and does not pass it on to SpamSieve for analysis.
- Added support for Growl notifications via Gntp (requires Mac OS X 10.7 or later).
- SpamSieve is better at handling file permission errors.
- SpamSieve is better at handling errors when running helper tools.
- Improved SpamSieve’s ability to still function when the application package is damaged.
- Added the **AddStandardRules esoteric preference**, which lets you prevent SpamSieve from creating its built-in blocklist and whitelist rules if you prefer to manage the rules yourself.
- Fixed a bug that could reduce SpamSieve’s filtering accuracy for some messages with attached files.
- Made various improvements to the documentation.
- Updated the German localization.

### 2.8.8—November 17, 2011

- Improved compatibility with pre-release versions of Mac OS X.
- Added support for [Postbox](#)<sup>147</sup> 3.0.
- Added support for [Growl](#)<sup>148</sup> 1.3.
- Made various changes to improve SpamSieve’s filtering accuracy.
- The [Exclude my addresses](#) feature now lets you specify additional addresses via Terminal, if you don’t want to clutter your “Me” card in Address Book.
- The Apple Mail plug-in installer is more resilient to permissions errors.
- Added [example](#) of using colored flags to sort spam messages in Apple Mail by spamminess.
- Added some logging to detect obscure errors when loading SpamSieve’s Apple Mail plug-in.

<sup>145</sup><http://www.apple.com/macosx/mountain-lion/security.html>

<sup>146</sup><http://erikhinterbichler.com/software/herald/>

<sup>147</sup><http://www.postbox-inc.com>

<sup>148</sup><http://growl.info>



- Improved the French localization.

### 2.8.7—August 31, 2011

- Improved compatibility with pre-release versions of Mac OS X.
- Made various changes to improve SpamSieve’s filtering accuracy.
- SpamSieve now runs as a 64-bit application on Mac OS X 10.7 Lion. This allows for faster launch times and reduced overall system memory use if you are running exclusively 64-bit applications. It also prevents problems caused by buggy input manager haxies. You can use the Finder’s **Get Info** window to set SpamSieve to run in 32-bit mode if you want to play classic Mac OS notification sounds or to reduce the memory use of SpamSieve itself.
- When training an Apple Mail message in the **Spam** mailbox as good, SpamSieve is now better able to match it up with the proper inbox.
- Offloaded more PDF processing to the helper tool so that SpamSieve itself doesn’t crash if you receive a message with a corrupt PDF attachment.
- Made the Apple Mail plug-in installer more robust and better at reporting errors.
- An error finding the built-in copy of SpamSieve’s Eudora plug-in will no longer prevent SpamSieve from launching, unless it actually needs to install the plug-in.
- Entourage is supposed to create the **Entourage Script Menu Items** folder, but for extra robustness SpamSieve will now create it if it’s missing.
- If SpamSieve’s PDF reader detects that the CTLoader input manager is loaded, it now logs a warning that this may cause SpamSieve to hang.
- Tried to work around an unconfirmed issue that could prevent SpamSieve from processing the first few Apple Mail messages on Mac OS X 10.7 Lion.
- Fixed a bug with re-personalizing the application via URL.
- Clarified the [Do an Initial Training](#) section of the manual.
- Updated the [Import Addresses...](#) instructions for Microsoft Outlook.
- The [Setting Up a Spam Filtering Drone](#) section of the manual now includes instructions for setting up a drone for multiple mail accounts.
- The manual now explains how to open the **Library** folder on Mac OS X 10.7 Lion.

### 2.8.6—July 6, 2011

- Made various changes to improve SpamSieve’s filtering accuracy.
- Improved compatibility with Mac OS X 10.7 (Lion).
- Added support for [Postbox 2.5](#)<sup>149</sup>.
- Updated the [Setting Up MailMate](#) instructions for the new preferences in MailMate 1.1.2.
- Updated the [Setting Up Outlook 2011](#) instructions for Microsoft Office 2011 Service Pack 1.
- Updated the [Setting Up Postbox](#) instructions to ensure that messages that you train as spam are moved to the junk mailbox or trash.
- Worked around a rare OS/hardware condition that could prevent SpamSieve from launching.
- The Apple Mail plug-in is better at reporting errors when it’s unable to fully load itself.
- Made various other clarifications to the manual.
- Adjusted the help page titles to fit better in the menu and search results.

---

<sup>149</sup><http://www.postbox-inc.com>



### 2.8.5—March 1, 2011

- Improved SpamSieve’s filtering accuracy.
- Improved compatibility with the Thunderbolt MacBook Pros and pre-release versions of Mac OS X.
- Freron Software’s [MailMate](#)<sup>150</sup> now works with SpamSieve, as described in the [Setting Up MailMate](#) section of the manual.
- [Whitelisting Previous Recipients](#) now works with Microsoft Outlook 2011.
- The **Train as Good** command can now move spam messages out of the spam folder when running a localized version of Microsoft Outlook 2011.
- SpamSieve’s Apple Mail plug-in helper now runs as 64-bit on Mac OS X 10.6, where possible, to prevent input manager haxies from interfering with the training commands.
- Added a workaround to prevent SpamSieve from hanging if the address book database is damaged.
- Clarified the text in the **Welcome** and **Purchase** windows.
- Improved the instructions for using Microsoft Outlook and Entourage with Exchange accounts.
- Updated the [Setting Up Postbox](#) section of the manual.
- Made various improvements to the documentation.
- Updated the Danish and Spanish localizations.

### 2.8.4—October 13, 2010

- SpamSieve now integrates with [Microsoft Outlook 2011](#)<sup>151</sup>. For more information, see the [Setting Up Outlook 2011](#) section of the manual.
- SpamSieve now integrates with [Postbox](#)<sup>152</sup>, an enhanced version of Thunderbird. For more information, see the [Setting Up Postbox](#) section of the manual.
- Adjusted SpamSieve’s tokenizer to improve the filtering accuracy.
- The **Train as Good** command in Apple Mail is better at moving messages in the spam folder or trash back to the inbox.
- Fixed a regression where the whitelist and blocklist windows wouldn’t open when running SpamSieve under certain localizations.
- Improved the localizations.

### 2.8.3—August 31, 2010

- Adjusted SpamSieve’s tokenizer to improve the filtering accuracy.
- Improved compatibility with pre-release versions of Apple Mail.
- [MailForge](#)<sup>153</sup> now works with SpamSieve, as described in the [Setting Up MailForge](#) section of the manual.
- Made some changes to better support the upcoming Microsoft Outlook 2011. (Full support will come when Office ships.)
- Added various updates and clarifications to the manual.
- Fixed a regression where SpamSieve wouldn’t be able to install its Apple Mail plug-in if Mail’s folder had been redirected using an alias.

---

<sup>150</sup><http://freron.com>

<sup>151</sup><http://www.microsoft.com/mac/office2011features/office2011.msp>

<sup>152</sup><http://www.postbox-inc.com>

<sup>153</sup><http://www.infinitydatasystems.com/mailforge/>

- Fixed a bug where SpamSieve would sometimes quit when coming out of trial mode.
- Fixed a bug where sometimes the **Hits** column in a rules window couldn't be resized.
- Worked around an OS bug that could cause an internal error when reporting a corpus error.
- Made various modernizations to SpamSieve's code and interface files.
- The Apple Mail plug-in now shows up with the proper name in [Mail Plugin Manager](#)<sup>154</sup>.
- Updated the disk image layout.

### 2.8.2—May 25, 2010

- Improved compatibility with pre-release versions of Mac OS X.
- Added Dutch, Italian, and Swedish localizations.
- Made various code improvements and modernizations.
- SpamSieve is better able to recover from certain types of damaged corpus files.
- Updated the “Setting Up Eudora” section of the manual.
- Improved the layout of the [Software Update...](#) window.
- Adjusted the packaging of the disk image and the installation instructions.
- Fixed a bug that could cause a crash when parsing messages with an invalid Date header.
- Fixed a regression where SpamSieve would sometimes bring up an alert sheet to report that you already had the latest version.
- Fixed a crash in the software updater.

### 2.8.1—March 24, 2010

- Fixed a regression in the SQLite build that could cause SpamSieve to crash when running on a PowerPC-based Mac.

### 2.8—March 24, 2010

- Made various changes to improve SpamSieve's filtering accuracy.
- Adjusted the **SpamSieve - Train as Good** command in Apple Mail to reduce confusion. Training a message as good now will only move the message into the inbox of an *enabled* account. If no account matches the message or if the proper account is disabled, it will move the message into the inbox of the first enabled account (even if it doesn't match). Thus, the message will always move out of the **Spam** mailbox, and it will no longer seem to disappear because it was moved into an inbox that was hidden.
- Made various code modernizations.
- Apple Mail now auto-launches SpamSieve sooner, to speed up the filtering of the first messages.
- Improved the support for server-side **Spam** mailboxes in Apple Mail.
- Clarified the instructions in the [Do an Initial Training](#) section of the manual.
- Added the [How do I make SpamSieve catch spams sent from my own address?](#) section to the manual.
- Expanded the [Correct All Mistakes](#) section of the manual.
- Improved the Apple Mail troubleshooting instructions.
- Improved the styling of the Apple Help.
- Improved SpamSieve's launching speed.

---

<sup>154</sup><http://github.com/aaronharnly/Mail-Plugin-Manager>

- Fixed a bug where, in rare circumstances, SpamSieve didn't filter all of the first batch of messages when using Apple Mail on Mac OS X 10.6.
- SpamSieve will now warn you if it looks like its Apple Mail plug-in has been damaged by an application slimming utility. This could lead to Mail continually reporting that the plug-in was incompatible.
- SpamSieve will now complain if it looks like you've manually installed the Apple Mail plug-in in the wrong folder instead of using SpamSieve's installer.
- Made a change to try to work around a bug in Apple Mail that could make training a message as good create a duplicate copy of the message.
- Improved the **Purchase** window to reduce confusion about the demo period, serial numbers, and the number of seats that you've purchased.
- Modernized the **Software Update** window and code.
- Changed the way the **Software Update** feature finds the downloads folder on Mac OS X 10.5 and later because sometimes the one that Internet Config returned would be invalid or unwanted.
- Fixed a bug where SpamSieve would crash when processing certain invalid URLs.
- Fixed an error where a newly added whitelist/blocklist rule might not be auto-selected.
- Removed the Dutch, Italian, and Portuguese localizations because they were out of date. If you would like to update the translation for one of these languages, please contact [spamsieve@c-command.com](mailto:spamsieve@c-command.com)<sup>155</sup>.

#### 2.7.7—October 20, 2009

- Improved compatibility with pre-release versions of Mac OS X.
- Made some changes to improve SpamSieve's filtering accuracy.
- Fixed a bug where the "Train as Good" command in Apple Mail didn't move Exchange messages back to the inbox.
- [Encoded HTML mail is spam](#) is now off by default, to reduce the number of false positives.
- Modernized the code.
- Updated the Vietnamese localization.
- Updated the [Apple Mail script for discarding spam](#).

#### 2.7.6—September 9, 2009

- Improved compatibility with pre-release versions of Mac OS X.
- Expanded the [Can I delete spam messages that are in the spam folder?](#) section of the manual.
- Fixed a bug in the [Setting Up a Spam Filtering Drone](#) instructions.
- Improved number entry in the corpus window.
- Improved the reporting of unexpected errors.
- Updated links to indicate that [Mailsmith](#)<sup>156</sup> is now available from Stickshift Software.
- Added a Console warning if the Apple Mail plug-in detects that CTLoader is installed.
- The crash reporter works better with Mac OS X 10.6.
- Fixed a mistake in the French localization.

#### 2.7.5—July 29, 2009

---

<sup>155</sup><mailto:spamsieve@c-command.com>

<sup>156</sup><http://www.mailsmith.org>

- Made various accuracy improvements.
- Fixed a problem where Apple Mail (running on pre-release versions of Mac OS X 10.6) could freeze at launch if you had a rule involving address book groups.
- Rewrote the [Setting Up a Spam Filtering Drone](#) instructions.
- Added [Why does the Spam mailbox in Apple Mail appear empty even though there's a number beside it?](#) to the frequently asked questions.
- Updated the [Automatically Deleting Old Spam Messages](#) instructions to include Entourage.
- The search fields are now scrollable.
- The Apple Mail plug-in is better at detecting when SpamSieve's Dock icon is hidden.
- Worked around a problem where Mail could crash if you had installed two copies of the SpamSieve plug-in at the same time.
- Fixed a bug that could cause SpamSieve to freeze when applying a whitelist/blocklist rule involving certain regular expressions.
- The crash reporter works better with pre-release versions of Mac OS X 10.6 (Snow Leopard).
- Fixed a bug that could prevent SpamSieve from launching.
- Updated the Dutch, Japanese, and Korean localizations.

#### 2.7.4—April 13, 2009

- Improved compatibility with pre-release versions of Mac OS X 10.6 (Snow Leopard).
- SpamSieve is better able to recover from corpus files that were damaged due to disk errors.
- Improved the Entourage installer's error handling.
- Improved the error reporting when saving the corpus.
- Improved the troubleshooting instructions.
- Fixed a problem where messages trained as good in Apple Mail could be moved into the inbox of a disabled account.
- Fixed a bug that could cause harmless error messages to be logged to the Console when playing System 7 sound files.
- The crash reporter now warns before sending a report without an e-mail address.
- You can now press Enter to click the **Send Report** button in the crash reporter.

#### 2.7.3—January 26, 2009

- Rewrote and restructured the manual to make the setup and troubleshooting instructions clearer.
- Replaced the **Training Tip** window with an alert that's displayed when SpamSieve's corpus is empty. This goes along with the more explicit guidance that ongoing training is only necessary to correct mistakes.
- The Entourage installer no longer asks before replacing existing script files. If you want to customize the scripts (rare these days, since there are so many built-in configuration options), you should use copies with different names to avoid having SpamSieve overwrite them.
- Changed the recommended Entourage rule setup to better handle uncertain messages. The installer now creates the **Uncertain Junk** category if necessary.
- Made the Apple Mail plug-in installer more robust.
- Worked around a problem parsing certain multipart messages.
- Adjusted the built-in blocklist rules for better accuracy.

- Reduced memory usage when processing message attachments.
- Fixed a bug sorting in rules windows.
- Fixed a bug marking incoming Entourage messages as Uncertain Junk.
- Updated the localizations.

### 2.7.2—October 29, 2008

- Made various accuracy improvements.
- Improved compatibility with pre-release versions of Mac OS X 10.6 (Snow Leopard). There are now two separate versions of SpamSieve's Apple Mail plug-in. Version 1.3 is for Mac OS X 10.4; version 1.4 is for Mac OS X 10.5 and later. SpamSieve will auto-choose which one to install (or update) based on the version of Mac OS X that you're running.
- Added new sections to the manual about [Whitelisting Previous Recipients](#) and [iPhone Spam Filtering](#). Expanded the [Auto-train with incoming mail](#) section.
- Worked around a problem where the [Edit Log](#) command would try to open SpamSieve's log using Script Editor if Launch Services was confused.
- Rewrote filesystem code to improve performance and error reporting.
- If there's an error getting the downloads folder for a software update, SpamSieve now defaults to **Downloads** rather than **Desktop**.
- Worked around a problem where training (using Apple Mail on Mac OS X 10.5) could be interrupted.
- Added Korean localization.
- Moved **.nib** files that don't need localization out of the **English.lproj** folder. This should make it easier to run SpamSieve in a language other than English without changing the default language on your Mac.
- Fixed some small memory leaks.
- Improved reporting of unexpected errors.
- Added placeholder text to the [Purchase...](#) window.
- Added **Help** button to the **Software Update** window.

### 2.7.1—June 4, 2008

- Fixed a regression in version 2.7 where SpamSieve was slow loading certain large corpus files when running on Mac OS X 10.5.
- Worked around a bug in Mac OS X 10.4 that could cause a crash when training a message with Apple Mail.
- Made some minor accuracy improvements.

### 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.

#### 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 phishing 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](#)<sup>157</sup>.
- 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.
- 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](#) SpamSieve or get a [serial number reminder](#).
- 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.

---

<sup>157</sup><http://www.apple.com/universal/>

- 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.
- 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](#) 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.
- 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 SpamSieve 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](#) 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](#) that lets you open SpamSieve's windows if its Dock icon is hidden (and thus the menu bar 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](#).
  - 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 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.
- 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](#). 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](#), and SpamSieve now supports AppleScript Kit terminology.
  - 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 flash when new good messages arrive.
  - Now supports System 7-format notification sounds as well as [Entourage sound sets](#)<sup>158</sup>. 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.
  - Added new scripting verb `add entourage addresses`. This will allow you to [keep the Entourage addresses in sync](#) by using an Entourage shutdown schedule.
  - Can automatically [add the recipients](#) 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](#) 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.

---

<sup>158</sup><http://www.soundsetcentral.com>

- Mailsmith Integration
  - Can automatically [add the recipients](#) of the messages you send to the whitelist.
- PowerMail Integration
  - Can automatically [add the recipients](#) 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 for discussion of SpamSieve.
  - 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 message'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 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.
- The history and the corpus files 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 Eudora 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 Eudora 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.