



Simply better network security.™



## SpamFilter

Unsolicited commercial email (commonly referred to as *spam*) is an increasing problem for businesses that use Internet email. Spam consumes expensive Internet bandwidth and wastes users' time reading and deleting unwanted messages.

eSoft's *SpamFilter* helps to reduce the amount spam and unwanted email passed through your system using advanced spam filtering technologies.

---

### Copyright Notices

eSoft, Inc. 2007. eSoft, TheatWall and InstaGate are registered trademarks and DIA, SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft, Windows and Outlook are registered trademarks of Microsoft Corporation.

Portions of InstaGate's software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

# Configuring SpamFilter

*SpamFilter* identifies spam by performing a variety of spam recognition tests on each incoming message. The test results are used to determine the likelihood a message is spam. Messages identified as spam can be instantly deleted, forwarded to the Spam Quarantine for review, or simply marked as spam and passed on to the recipient.

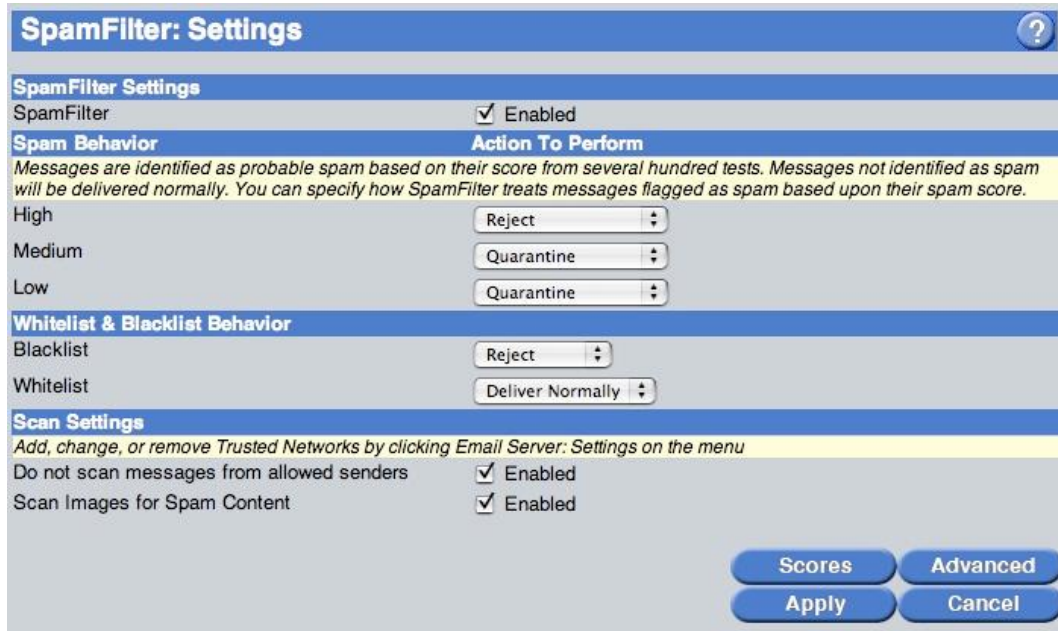
---

**Note:** You must configure the Email Server Settings before enabling *SpamFilter*. Click the *Online Help* link in the lower left corner of the administrative interface to access the *Email Server* help files.

---

To configure *SpamFilter*:

1. Select *Settings* from the *SpamFilter* menu.
2. Select the *SpamFilter Enabled* check box.



3. All messages identified as spam are assigned a *Score* based on the results of various spam recognition tests. Although spam filtering is not an exact science and therefore not 100% guaranteed, messages that appear extremely likely to be spam are assigned a *High* level rating. Messages that are likely to be spam, but may also be legitimate email are assigned a *Medium* spam level rating. Messages that are only slightly more likely to be spam than legitimate email are assigned a *Low* spam level rating.

---

**Note:** To modify the Spam Level thresholds, click *Advanced*.

---

For each spam level, you must then select the *Action to Perform*:

- **Deliver Normally** — Simply marks messages as spam and passes them on to the intended recipient. This is the least disruptive method of managing email with *SpamFilter*. In this mode, the following header is added to each message identified as spam prior to delivering it to the intended recipient:

**X-Spam-Flag: Yes**

Users can then set up their email applications to filter messages containing this header.

Refer to the documentation included with your email application for information on filtering mail.

- **Quarantine** — Marks messages as spam and forwards them to the Spam Quarantine. This is the most common method of managing email with *SpamFilter*, as it ensures valid email is delivered by allowing the administrator or user to review marked messages to determine if they are spam.
- **Accept and Delete** — Accepts the messages from the sender and silently discards them. The sender will never know their message was not received. *Accept and Delete* and *Reject* are the easiest and most aggressive methods of managing email with *SpamFilter*. Selecting this option may result in the deletion of some legitimate (non-spam) mail.
- **Reject** — Rejects messages from the remote sender so the messages are not accepted. This is the easiest and most aggressive method of managing email with *SpamFilter*. Selecting this option may result in the rejection of some legitimate mail.

---

**Note:** Consider the number of users on your system and the amount of spam they receive when selecting the action to perform. If the numbers are large, manually reviewing and releasing legitimate email (false-positives) from the SpamFilter Quarantine may prove too daunting a task to perform on a regular basis. Remember, false-positives can occur at any time and may be extremely urgent messages. You should only select this option if you are willing and able to review messages in the *Spam Quarantine* often enough that urgency is still possible.

---

4. Select the behaviour you want performed on messages that match addresses stored in the Whitelist and Blacklist databases. You may choose *Reject* or *Quarantine* for *Blacklists* and *Quarantine* or *Deliver Normally* for *Whitelists*.
5. Check the *Do not scan messages from allowed senders Enabled* check box to prevent SpamFilter from scanning messages sent from IP addresses in the trusted networks list. The trusted networks list, specified in Email Server Settings, consists of specific trusted networks. Connections which authenticate through SMTP are also exempt. SMTP Authentication is enabled by default, but can be disabled in the Email Server Settings Advanced page by unchecking *Allow Client Authentication*.
6. Check the *Scan Images for Spam Content* to enable Optical Character Recognition (OCR) features in *SpamFilter*. *NOTE: SpamFilter reads content from the follow image formats: jpg, gif, animated gif, png, pnm, ppm, pgm and bmp.*
7. To override default scores assigned for tests performed by *SpamFilter* click the Scores button.
8. To configure advanced SpamFilter settings (such as, adjusting the Spam Level thresholds) click the Advanced button.
9. Click *Apply* to save your settings, or *Cancel* to exit without saving.

# Configuring Advanced SpamFilter Settings

*SpamFilter* provides several advanced configuration options allowing you to customize the product to fit your needs.

To configure the advanced *SpamFilter* settings:

1. Click the *Advanced* button in the *SpamFilter Settings* form.
2. *SpamFilter* compares each email message to a set of rules that define various characteristics of spam. Each of these rules is given a value (score) representing its spam likeliness. For example, if the "From:" header has illegal characters, that might score 4 points. If the "Subject:" line contains the word VIAGRA, that might score 2.8 points. The sum of all tests results in the score assigned to the message. The default thresholds for each Spam Level are provided by eSoft. To customize the *Threshold Settings*, enter the threshold values.

**SpamFilter: Settings: Advanced** ?

**Spam Probability Threshold Settings**  
Each message is assigned a score based on its performance on several hundred tests. Messages that score lower than the value entered for Low are not marked as spam. Use the fields below to change how spam probabilities are assigned.

Low	<input type="text" value="5"/>
Medium	<input type="text" value="10"/>
High	<input type="text" value="17"/>

**Defaults**

**Update Settings**

Last Update	Wednesday 15th, August 2007 01:42:03 AM
-------------	---

**Update Now**

**DIA Settings**

DIA Reputation Filter	<input checked="" type="checkbox"/> Enabled
Reject From DIA Real-Time Blacklist	<input checked="" type="checkbox"/> Enabled

**Historical Averaging Settings**

Use historical averaging to rate individual senders	<input checked="" type="checkbox"/> Enabled
---	---

**Reset DB**

**Other Settings**

Maximum message size to scan	<input type="text" value="200"/> kB
Add detailed report to message headers	<input type="checkbox"/> Enabled
Add indicator to message subject	<input type="checkbox"/> Enabled
Use extended rules	<input checked="" type="checkbox"/> Enabled
All mail comes from one server	<input type="checkbox"/> Enabled

**Apply** **Cancel**

3. eSoft maintains the list of spam rules and provides updates as necessary. The new rules are downloaded nightly at 1am. However, you may also update the list manually by clicking *Update Now* button.
4. Distributed Intelligence Architecture (DIA) is a system that is used by eSoft customers to provide information about attacks it is seeing. *DIA Reputation Filter* is a feature that reports the score and source IP address of a message. It also received the average score seen by all other units around the globe. This is a useful feature to eliminate spam messages sent from known spammers and bot networks.
5. DIA also supports RBLs based from reports received through *SpamFilter*. These lists are created by selecting IP addresses that are clearly the source of spam. Enabling *Reject from DIA Real-Time Black List* allows *SpamFilter* to reject any message from IP addresses found in DIA's RBL list reducing the need to process those messages through *SpamFilter's* spam engine.
6. If you wish to use historical averaging, select the *Use Historical Averaging to Rate Individual Senders* checkbox. This will add points to a message or remove them based on the score of the sender's previous messages.
7. In some cases you may choose to reset the database that controls *Historical Averaging*. To do this, click the *Reset DB* button.
8. Messages over a certain size are not scanned for spam to improve performance. Enter the maximum size (in KB) of messages that you wish to be scanned for spam in the *Maximum Message Size to Scan* text box or *unlimited* to scan everything.

9. Enabling *Add detailed report to message headers* will include a report that shows the result of all tests performed by *SpamFilter*. The report is placed in the headers section of the email message is not visible to most users unless their email client is configured to show the message headers. Enabling this feature is useful for gathering information about messages which can be used to fine tune *SpamFilter* scores and thresholds. If your mail clients have difficulty with the multi-line X-Spam-Report header, deselect the *Add Detailed Report to Message Headers Enabled* check box (not common).
10. If you elect to *Deliver Normally* to users for them to filter, select the *Add indicator to message subject Enabled* check box to add the word *SPAM* to the subject line of messages identified as spam. Users can then quickly identify spam messages without looking at the message headers.
11. SpamFilter uses an extensive set of spam recognition tests to identify spam. Occasionally, in low bandwidth or heavy load environments, running all these tests can create performance issues. To limit the number of tests performed on each message, deselect the *Use Extended Rules Enabled* check box.
12. If your system is in an environment where all email comes from the same IP address, you should enable the *All mail comes from one server* options and enter the IP Address of that server. This tells *SpamFilter* to ignore rules based on source address.
13. Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Modifying SpamFilter Test Scores

*SpamFilter* identifies spam by comparing each email message to a set of rules that define various characteristics of spam. Each of these rules is given score representing its spam likeliness. If a message matches a rule, the value assigned to the rule is added to the message's final score to determine the appropriate spam level rating.

eSoft maintains the list of spam rules and scores and provides updates as necessary. You can also update the spam rule scores manually. The ability to change scores allows you to turn up or turn down the sensitivity of any individual rule.

**SpamFilter: Settings: Test Scores**

**Test Scores**  
*SpamFilter applies hundreds of tests to every message. A message's spam probability score is increased or decreased by the score of each test. You can use the Defaults (recommended) or change the score for any individual test with Custom.*

Defaults  
 Custom

Group:

Rule	Ham Hits	Spam Hits	Default Score	Current Score
BAYES_00	—	—	-1.665	-1.665
BAYES_05	—	—	-0.925	-0.925
BAYES_20	—	—	-0.730	-0.730
BAYES_40	—	—	-0.276	-0.276
BAYES_50	—	—	3	3
BAYES_60	—	—	5	5
BAYES_80	—	—	11	11
BAYES_95	—	—	15	15
BAYES_99	—	—	20	20

Apply Cancel

To modify the spam rule scores:

1. Click the *Scores* button in the SpamFilter configuration page.
2. Select the *Custom* radio button.
3. Select the *Group* of rules you wish to modify from the drop-down list. All the rules for the selected group are listed.
4. To modify the score for a particular rule, enter the value you wish to assign to the rule in the *Current Score* text box.
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Configuring Bayesian Filtering

Bayesian Filtering allows you to train *SpamFilter* to determine which messages are likely to be spam or non-spam based on keyword content.

For example, suppose you receive a lot of messages that contain some variation on the term "free software" but don't quite score high enough to be marked as spam through other *SpamFilter* rules. If the Bayesian Filter has learned that messages containing the following text are likely to be spam:

- "Call today for FREE Software!"
- "Why don't you call today for free software?"
- "Your FREE SOFTWARE is waiting!"

Then it's likely to decide that a new message containing the text following text also as spam:

- "Want to download some absolutely free software TODAY?"

Determining the likely-hood of being spam will raise the message's score. Conversely, if it sees messages with content similar to those that you've identified as non-spam, it will lower score.

However, in order for Bayesian Filtering to determine a message's probability of being spam or non-spam, it must be trained in one or more of the following modes:

- *Automatic.* Bayesian Filtering can automatically learn messages as spam or non-spam based on their score from other SpamFilter rules. SpamFilter uses conservative values to make this determination so only the very lowest and very highest scored messages are candidates may be auto-learned.

On the other hand, messages deleted and released from the Quarantine are automatically learned regardless of the message's actual score. It is able to do this because you're making the decision whether a message is spam (deleted) or non-spam (released).

The advantage of automatic training is that it requires no work on your part other than normal Quarantine management.

- *Manual.* The second mode of training Bayesian Filtering is manual training it through your email clients. You must download and install the SpamFilter Add-In for Outlook 2000 and Outlook 2003. This Add-In allows you to mark selected messages as either spam or non-spam from Outlook 2000.

While this requires more work on your part, one advantage of manual training is that you'll populate the database much faster and you can even allow your employees to help. Another advantage is that by training from your corpus of messages, the database will be much more "in tune" to the kind of spam and non-spam your organization receives. You also receive all of the advantages of automatic training.

---

Note: In order for the SpamFilter Add-In to work, the product's administrative port must be reachable. If your product is behind a firewall and you have clients that you want to use it that are not behind the firewall, you'll need to make port 443 or 8001 available. Consult your firewall documentation on how to do this.

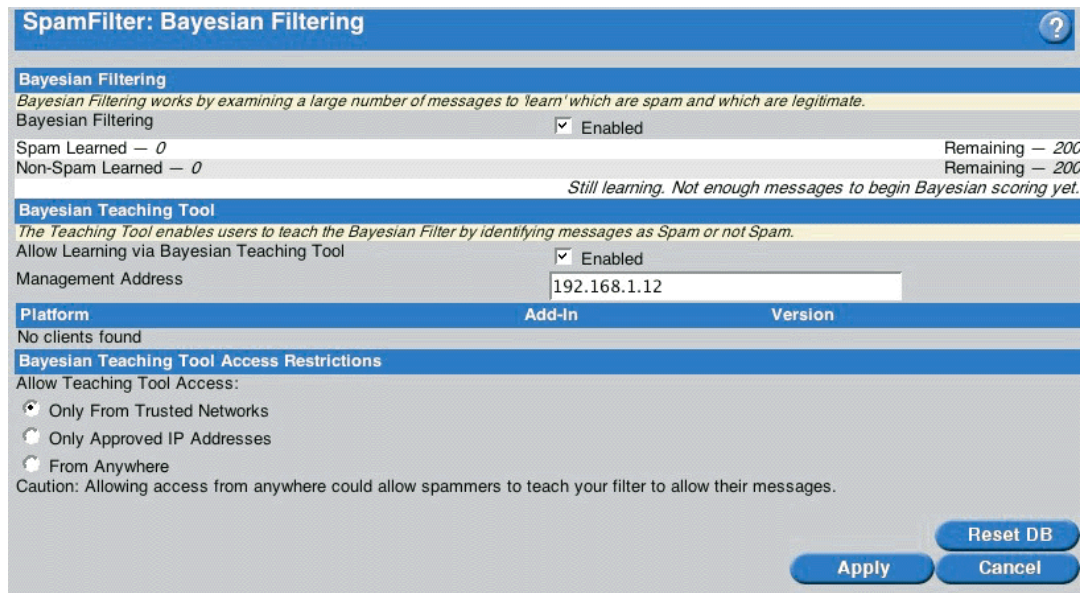
---

Once the Bayesian Filtering database has accumulated 200 spam and 200 non-spam messages, it will begin to score messages. Scoring is based on the probability of the message being spam or non-spam.

To configure Bayesian Filtering settings:

1. Select *Bayesian Filter* from the *SpamFilter* menu.
2. To enable automatic learning, select the *Bayesian Filtering* checkbox.

After enabling, you'll see a section that shows the status of the Bayesian Filtering database. You'll see how the number of spam and non-spam messages that have been learned from both automatic and manual modes and how many more must be learned before Bayesian Filtering starts adding its score to messages.



3. To enable manual learning, select the *Allow Learning via Bayesian Teaching Tool* checkbox.

After enabling, you'll see an additional configuration section to control how clients are managed.

4. The *Management Address* is added to message headers and is used by the SpamFilter Add-In for Outlook to determine the address it should contact. By default it uses one of your product's IP addresses, but you may need to change this if you are behind a firewall or wish to use a domain name.
5. SpamFilter stores a database of messages to aid in manual management. You can control how the database size by changing the *Number of Days to Retain* and the *Maximum Allowable Disk Space*. The latter value is in gigabytes of hard drive space. Automatic maintenance of the database is determined by whichever of these values are reached first.

For example, if you've configured *Number of Days to Retain* for 7 days and *Maximum Allowable Disk Space* for 30 GB, on the 8th day messages from the first day will be deleted regardless of whether the database has reached 30 days.

If a client marks a message that is not in the database, it will still be learned, but it may not accurately update the Bayesian Filtering database to correct the auto-learn value it received coming in. For example, it is possible for a message to be auto-learned as not-spam, but if the message is marked as spam but is not in the database, the score is nullified. If the message was in the database, the score would be marked as spam.

6. To control the access of clients that may access the server, change the *Bayesian Teaching Tool Access Restrictions* setting. By default this is set to *Only From Trusted Networks*. The possible options are:

- *Only From Trusted Networks.* Only clients from the networks defined by your Email Server/Relay *Mail Client Access Settings* (see Configuring the Email Server/Relay Advanced Options) can train the Bayesian database.
- *Only Approved IP Addresses.* This allows you to specify IP addresses and networks that may use clients.

The format is either *network/bits* or *ip address*. For example, if you want to only allow addresses on your network and a few home clients, you might specify the approved addresses as:

192.168.1.0/24

64.12.32.23

82.21.23.121

- *From Anywhere.* Anyone can teach the Bayesian Filter.

7. Under normal operating conditions, you should not have to reset the Bayesian database. If you reset the Bayesian database, you will need to retrain it through automatic or manual learning.

---

Note: If you have a system backup that includes SpamFilter files, you can restore the database to a previous state. Simply restore all files beginning with *bayes*.

---

8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Reset Bayesian Database

Under normal operating conditions, you should not have to reset the Bayesian database. If you reset the Bayesian database, you will need to retrain it through automatic or manual learning. However, some circumstances may warrant it, like acquiring new domains with different mail characteristics.

---

Note: If you have a system backup that includes SpamFilter files, you can restore the database to a previous state. Simply restore all files beginning with *bayes*.

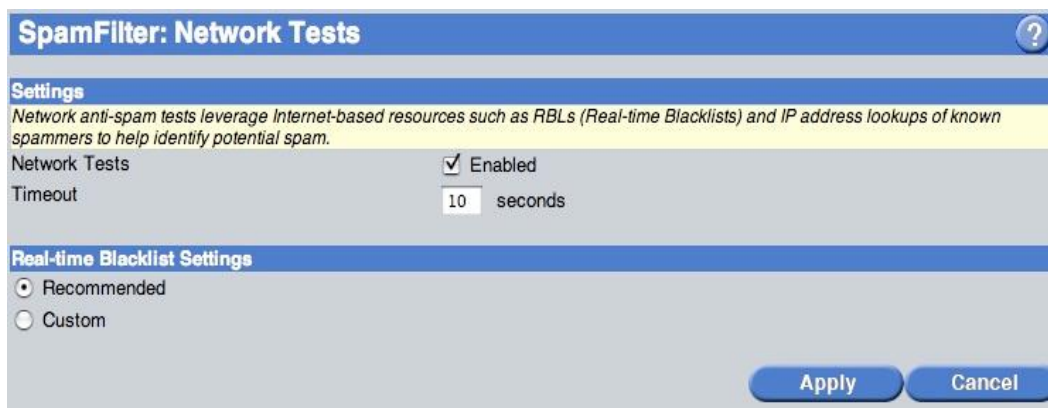
---

## Configuring Network Tests

*Network Tests* allows *SpamFilter* to leverage external services, such as real-time blacklists (RBLs) and IP address databases of known spammers and systems that are compromised/mis-configured systems. These tests are helpful for identifying potential spam and contribute to the scoring values assigned to each incoming message.

To configure *Network Tests*:

1. Select *Network Tests* from the *SpamFilter* menu.
2. Select the *Enabled Network Tests* checkbox to enable these tests.



The screenshot shows a dialog box titled "SpamFilter: Network Tests". It has a blue header bar with a question mark icon on the right. Below the header is a "Settings" section with a yellow background containing the text: "Network anti-spam tests leverage Internet-based resources such as RBLs (Real-time Blacklists) and IP address lookups of known spammers to help identify potential spam." Underneath, there is a "Network Tests" checkbox which is checked and labeled "Enabled". Below that is a "Timeout" field with a text input containing "10" and the unit "seconds". A "Real-time Blacklist Settings" section follows, with two radio buttons: "Recommended" (which is selected) and "Custom". At the bottom right of the dialog are two buttons: "Apply" and "Cancel".

3. Real-time Blacklist Settings can be modified to allow you to specify which RBLs *SpamFilter* will use. To select from the list of available RBL, click the *Custom* radio button and select the lists you wish to use. *NOTE: Adding RBLs can adversely affect system performance and may also increase the false positive rate.*
4. Click Apply to save your settings, or Cancel to exit without saving.

## Adding Custom Rules

*SpamFilter* supports the capability to assign scores to certain keywords or phrases. The scores assigned to custom rules are added to the total score assigned to incoming messages by *SpamFilter*. For example, if you want to prevent offensive words from reaching your users you could add those words to the custom rules with a high score. *SpamFilter* will add those scores to other tests and take the action defined in the *SpamFilter Settings* form. Conversely you could add keywords or phrases you want to pass through *SpamFilter*.

To add *Custom Rules*:

1. Click *Custom Rules* from the *SpamFilter* menu.

The screenshot shows a dialog box titled "SpamFilter: Custom Rules". It is split into two main sections. The top section, "Spam Rules", has a blue header and contains a "Spam Rules" label with a checked "Enabled" checkbox, a "Score" field with the value "200", and a "Keywords" text area containing the text "Viagra", "Free drugs", and "super deals from Cozko". The bottom section, "Non-Spam Rules", has a blue header and contains a "Non-Spam Rules" label with an unchecked "Enabled" checkbox. At the bottom right of the dialog are "Apply" and "Cancel" buttons.

2. If you wish to create a *Custom Rule* that increases the spam score, making the message more likely to be marked as spam, click the *Enabled Spam rules* checkbox.
  1. Enter a value in the *Score* field. This value will be added to all the other tests performed by *SpamFilter*. The action defined in *SpamFilter Settings* will be taken on the final score applied to the message.
  2. Enter the *Keywords* to match on for this rule. Each line in this field will be considered a unique keyword used to match. *NOTE: You may use standard words or regular expressions (regex) to create your patterns.*
3. If you wish to create a *Custom Rule* that reduces the spam score making the message less likely to be marked as spam, click the *Enabled Non-Spam rules* checkbox.
  1. Enter a value in the *Score* field. This value will be subtracted from all the sum other tests performed *SpamFilter*. The action defined in *SpamFilter Settings* will be taken on the final score applied to the message.
  2. Enter the *Keywords* to match on for this rule. Each line in this field will be considered a unique keyword used to match. *NOTE: You may use standard words or regular expressions (regex) to create your patterns.*
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.



## Regular Expression Example

test	<p>This is the simplest kind of regular expression. Each character matches a character in the text. This expression will match "test", but will not match "tester", "contest", "tes" or "best".</p> <p>Note: The keyword entries are automatically modified to only match at the beginning and ending of words. The next example will show you how to match partial words.</p>
*test.*	<p>A "dot", also known as a period or full stop, will match any character. The asterisk, or "star" will match any number of the previous character, or none at all. This expression will match "test", "tester" and "contest", as well as "The test was given and all students passed."</p>
[0-9]{3}-[0-9]{2}-[0-9]{4}	<p>This expression matches a U.S. Social Security number. The "[0-9]" is a character class. It will match anything from 0 to 9. The "{3}" means to match the previous character or character class 3 times. The dash following "{3}" is just a dash to match a dash. This example will match 111-222-3333, but not 1112223333.</p>
[0-9]{3}?.?[0-9]{2}?.?[0-9]{4}	<p>This expression is similar to the expression above, except it does not require a dash between parts of the U.S. Social Security number. The "." will match any character and the "?" matches the previous character zero or one time. This example will match 111-222-3333, 111.222.3333, 111*222*3333 and 1112223333</p>
(Fred Joe Mary).*Herbert	<p>The parenthesis start a group. The "vertical bar" character between the names Fred, Joe and Mary will match one of the choices. This expression will match any line that contains Fred, Joe or Mary, followed by Herbert on the same line.</p>

## Configuring Whitelists

The biggest problem with spam filtering is the so-called *false-positive*. This is a message that is "legitimate" meaning that it is supposed to get through, but because it possesses certain spam characteristics is marked as spam.

The key to reducing false-positives is the *Whitelist*. By adding an email address to the *Whitelist*, email messages sent to or from the address are automatically passed through *SpamFilter*, even if the messages are identified as spam. *Whitelists* can apply to entire domains or individual addresses. *SpamFilter* also maintains *Whitelists* for the system (called the global whitelist) and for individual users on the system.

You can identify addresses to add to the exception list by monitoring "caught" messages in the Spam Quarantine. If you select *Quarantine* from the *SpamFilter* menu, you can view all caught messages, locate any false-positives, release the messages to their intended recipients, and add the senders to the whitelist. This is not possible if you select *Delete* without delivering, however, as caught messages are deleted before the sender can be identified.

When you release a message from Quarantine, SpamFilter analyzes the message and provides suggestions to add to the white list. Simply review the suggestions listed, remove any addresses you do not wish to add, and click *Apply*.

Another option to consider is whether you should allow the entire domain or just the single specific address. The rule of thumb recommended is if the domain is from a site you know offers free mail, such as hotmail.com or yahoo.com, just enter the address. Otherwise, add the entire domain. For example, if *john@hotmail.com* sent a message to one of your users, you probably want to receive messages from john, but not other messages from the hotmail.com domain. Therefore, add **john@hotmail.com** to the white list. On the other hand, if *frank@franks-hotdogs.com* is a repeat customer whose coworkers might also send you messages, add the entire domain (**franks-hotdogs.com**).

For some situations, it may be desirable to create exceptions for entire domains, but restrict individual addresses. For example, you could create an exception for *goodsite.com*, but create a Blacklist for *badguy@goodsite.com*. In this case, email for every address in *goodsite.com* would be passed correctly through your system except for mail addressed to *badguy@goodsite.com*.



To set up an exception list:

1. Select *Whitelists* from the *SpamFilter* menu.
2. Select the *Whitelist* database you would like to modify. *Global* applies all matches to all users on the system.
3. Enter the domain names, IP addresses and email addresses you wish to add to the whitelist. Email messages sent to or from the addresses listed are automatically passed through SpamFilter, even if the messages are identified as spam.

If you enter an email address (for example, `jsmith@domain.com`), SpamFilter will pass-through any messages containing the email address in either the *To* or *From* fields. Therefore, if there is an email address in your domain for which you do not wish to filter out spam, simply enter the email address in the exception list.

---

**Note:** SpamFilter supports wildcards (\* and ?) when creating white or black lists. ? represents any single character. \* represents any number of characters including none at all.

For example, if you would like to accept mail from `john@hotmail.com` and deny all other `@hotmail.com` users, add `john@hotmail.com` to the white list, and `*@hotmail.com` to the black list. You can also do the opposite: black list `john@hotmail.com` and white list `*@hotmail.com` (only messages from john are denied). Other examples include: `*@*specials*` and `*offer*@*`.

---

3. The action used by *SpamFilter* matching the entries in the list are defined in the *SpamFilter Settings* form.
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Setting up a Blacklists

To automatically mark messages to or from a particular domain name or email address as spam:

1. Select *Blacklists* from the *SpamFilter* menu.
2. Enter the domain names and email addresses you wish to add to the blacklist. Email messages sent to or from the addresses listed are automatically rejected or quarantined based on the action defined in SpamFilter Settings.

---

**Note:** SpamFilter supports wildcards (\* and ?) when creating blacklists. "?" represents any single character. "\*" represents any number of characters including none at all.

For example, if you would like to accept mail from john@hotmail.com and deny all other @hotmail.com users, add `john@hotmail.com` to the whitelist, and `*@hotmail.com` to the blacklist. You can also do the opposite: blacklist john@hotmail.com and whitelist \*@hotmail.com (only messages from john are denied). Other examples include: `*@*specials*` and `*offer*@*`.

---

3. Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Viewing Messages in the Spam Quarantine

When you click the blue-highlighted text associated with a message in the Spam Quarantine, the View Message page appears in a separate window, displaying the message in its entirety. Inside the message, headers of interest, such as To, From, and Subject appear in bold.

To exit the View Message page and return to the Quarantine interface, click *Close*.

## Adding to Whitelists from the Spam Quarantine

When you release a message in the Spam Quarantine, *SpamFilter* analyzes the message and provides suggestions you may wish to add to the Whitelists. Simply review the suggestions listed, remove any addresses you do not wish to add and click *Apply*.

## Managing the Spam Quarantine

If you selected to Quarantine messages marked as spam in *SpamFilter Settings*, those messages can be viewed, deleted, and released using the Quarantine interface. *SpamFilter Quarantine* may be managed by the system administrator or configured to allow users to manage their own quarantine.

To manage messages via the *SpamFilter Quarantine*:

1. Select *Quarantine* from the *SpamFilter* menu.

---

**Note:** Administrators can access the Quarantine interface directly by going to the following URL:

**InstaGate**

`https://<ip address:8001>/EmailQuarantine`

**ThreatWall**

`https://<ip address>/EmailQuarantine`

---

1. You may limit the messages displayed in the *SpamFilter Quarantine* by selecting options in the *Show* section. There are three options for narrowing the lists of messages in the *SpamFilter Quarantine*.
  1. Select *All* displays all messages in the quarantine up to the number of messages specified in the page limit.
  2. Selecting *By date* allows you to specify the date of the messages you wish to view from *SpamFilter Quarantine*. The drop-down lists dates for all messages in the *SpamFilter Quarantine*. Select the date from the list you would like to view. The page will automatically refresh with only messages from the specified date up to the number of messages specified in the page limit field.
  3. Selecting *Search (All dates)* allows you to search the *SpamFilter Quarantine* for keywords in the To, From and Subject fields of all email stored in the *SpamFilter Quarantine*.
3. To sort the messages, simply click the appropriate column heading (*Date*, *Hits*, *From*, *To* or *Subject*).
4. To view a message, click the associated blue-highlighted text. The message in its entirety appears in a separate window. Inside the message, headers of interest, such as To, From, and Subject appear in bold.
5. To delete a message, select the message and click *Delete*.

To delete other messages in the *SpamFilter Quarantine* with the same *From*, *To* or *Subject* header as the selected message, select the appropriate check boxes at the bottom of the page, and click *Delete*. This deletes all applicable messages for the selected date. To apply the delete to all dates, you must select the *All Days* check box.

6. To release a message to the intended recipient, select the message and click *Release*.

---

**Note:** When you release a message in the *SpamFilter Quarantine*, *SpamFilter* analyzes the message and provides suggestions you may wish to add to the Whitelists. Simply review the suggestions listed, remove any addresses you do not wish to add, and click *Apply*.

---

7. To delete all messages in the *SpamFilter Quarantine*, click *Purge*.
8. Click *Settings* to configure the options for the quarantine.
9. Click *Done* to exit.

## Spam Quarantine Settings

The *SpamFilter Quarantine Settings* can be modified to control options such as where to send messages, who has access to the quarantine, how long messages remain in the quarantine and control over sending user notifications.

To access the *Spam Quarantine Settings*, click the *Settings* button in the Spam Quarantine form.

**SpamFilter: Quarantine: Settings**

**Quarantine Settings**

Destination  Local  
 Remote

**Local Management**

Access  Anyone who receives a notification or users with the permission: *Email*  
 Only users with permission: *Email*  
 Only system administrator

Automatically remove messages\* 7 Days / 1 GB Currently: <1 G / 32.73 G

**Local Notifications**

Recipients  All local addresses  
 Only users with permission: *Email*  
 Only the following addresses

Management address\* 192.168.1.1

When to send  Once every 1 Days  
 Immediately

Allow whitelisting from notification  Enabled

\*Settings are also used by: Email Content Filtering

**Apply** **Cancel**

### Quarantine Settings

If you selected Quarantine as the action to perform for any of the spam levels, you may specify the *Destination SpamFilter* sends those messages:

- **Local** — Messages marked as spam are saved locally and can be viewed, deleted, and released using the Quarantine interface. This is the recommended and default option.
- **Remote** — Messages marked as spam are forwarded to the specified email address. The address must be valid and have sufficient disk space available.

### Local Management

There are three different levels of quarantine access available in *SpamFilter*:

- **Anyone who receives a notification or users with the permission** — Users that receive a notification or have *Email* permission on *InstaGate* or are members of the *User Quarantine Management* group on *ThreatWall* will be able to access the Spam Quarantine. *NOTE: This option is useful when the mail server is configured to "Relay" and there are no users defined on the system.*
- **Only users with permission** — Only users with the *Email* permission on *InstaGate* or are members of the *User Quarantine Management* group on *ThreatWall* will be able to access the Spam Quarantine.

- **Only system administrator** — In this mode users do not have access to the spam quarantine. The system administrator must go through the quarantine to look for any potential false positives.

Every night, the Spam Quarantine will be analyzed. Messages older than the number of days set in the *Automatically remove messages* setting will be deleted automatically. You may also set the maximum size of the Spam Quarantine. Once *SpamFilter* reaches this threshold it removed the oldest messages until the size is reduced to below the threshold.

## Local Notification

*SpamFilter* can notify users on the system when messages are forwarded to the Spam Quarantine. You may configure this setting to limit who gets the notifications and how often they receive it.

To specify who receives the notifications select the *Recipients* from the following list:

- **All local addresses** — Any user that matches a defined email domain will receive notification.
- **Only users with permission** — Only users with the *Email* permission on *InstaGate* or are members of the *User Quarantine Management* group on *ThreatWall* will receive notifications.
- **Only the following addresses** — Email addresses entered into the list will receive a notification when spam is delivered to the quarantine. These users will have full access to quarantine.

Enter the Management Address. This is the IP address or host name that will be embedded in the notification message. When a user clicks on a link in the notification message, this is the address their web browser will connect to. Normally this will be the IP address of the management interface. However, in cases where the system is located behind a NAT firewall you may need to enter the external IP address so remote users have access to the quarantine.

Enter a number of hours or days for the Send email to users with messages in quarantine every option. This ranges from 1 hour to 30 days. You may also choose to send notifications immediately after message has been delivered to Spam Quarantine.

Check the *Allow whitelisting from notification messages Enabled* checkbox to allow recipients of the notification message to add senders to their personal *whitelists*.

After configuring the Spam Quarantine settings, click Apply to save your changes or Cancel to abandon them.

# Index

## A

Access	
Email Server.....	2
Quarantine.....	20
spam.....	21
Spam Quarantine .....	21
Spam Quarantine Settings .....	21
Access .....	2
Access .....	20
Access .....	21
Add Detailed Report.....	4
Advanced SpamFilter Settings	
Configuring.....	4
Advanced SpamFilter Settings.....	4
Allow Learning .....	7

## B

Bayesian Filtering	
Configuring.....	7
order.....	7
teach.....	7
training.....	7
Bayesian Filtering .....	7
Bayesian Teaching Tool checkbox .....	7
Blacklists .....	2, 17
Bot .....	4

## C

Changing	
Bayesian Teaching Tool Access Restrictions .	7
Changing.....	7
Check	
Scan Images.....	2
Check.....	2
Checkbox.....	12
Clicking	
Update Now.....	4
Clicking .....	4
Configuring	
Advanced SpamFilter Settings .....	4
Bayesian Filtering.....	7
Network Tests.....	11
Spam Quarantine .....	21
SpamFilter .....	2
Whitelists.....	15
Configuring.....	2
Configuring.....	4
Configuring.....	7
Configuring.....	11
Configuring.....	15
Configuring.....	21
Current Score.....	6

Custom Rules	False-positives .....	15
Adding .....	Firewall.....	7
Custom Rules .....	<b>K</b>	
<b>D</b>	Keywords	
Date, Hits .....	Enter.....	12
Deselect	Keywords .....	12
Add Detailed Report .....	<b>L</b>	
Use Extended Rules Enabled.....	Local Management.....	21
Deselect.....	Local Notification.....	21
Destination SpamFilter	Local Quarantine.....	2, 20
specify .....	Low spam.....	2
Destination SpamFilter.....	<b>M</b>	
DIA.....	Management Address	
DIA Real-Time Black List .....	Enter.....	21
DIA Reputation Filter.....	Management Address .....	7
<b>E</b>	Management Address .....	21
Email Server Settings .....	Managing	
Email Server/Relay Mail Client Access Settings .7	email.....	2
Enabled Network Tests checkbox	Spam Quarantine .....	20
Select .....	Managing .....	2
Enabled Network Tests checkbox.....	Managing .....	20
Enabled Non-Spam.....	Maximum Allowable Disk Space .....	7
Enabled Spam .....	Maximum Message Size .....	4
<b>F</b>	Medium spam.....	2
False-positives	Message Headers Enabled.....	4
reducing.....	Modify	
False-positives .....	Spam Level.....	2

SpamFilter Test Scores .....6

Modify .....2

Modify .....6

**N**

Network Tests

    Configuring .....11

Network Tests .....11

Non-spam .....2, 7

**O**

OCR .....2

Online Help .....2

Only

    Selecting.....20

Only .....20

Only .....21

Only Approved IP Addresses .....7

Only From Trusted Networks .....7

Optical Character Recognition .....2

Outlook

    SpamFilter Add-In .....7

Outlook.....7

**P**

Parts

    U.S. ....14

Parts .....14

Perform .....2

Purge .....20

**Q**

Quarantine

    access ..... 20

    SpamFilter Settings ..... 20

Quarantine .....2, 7, 15, 18

Quarantine ..... 20

Quarantine ..... 21

Quarantine Settings ..... 21

**R**

Rate Individual Senders checkbox

    Use Historical Averaging ..... 4

Rate Individual Senders checkbox..... 4

RBLs

    Adding ..... 11

RBLs ..... 4

RBLs ..... 11

RBLs SpamFilter ..... 11

Real-time Blacklist Settings..... 11

Reduces

    false-positives..... 15

    spam..... 12

Reduces..... 12

Reduces..... 15

Regular Expression Example ..... 14

Reject

    Enabling ..... 4

Reject..... 2

Reject.....	4	Select	
Relay.....	21	Action .....	2
Release.....	20	Add .....	4
Remember, false-positives.....	2	All Days .....	20
Remote — Messages .....	21	behaviour.....	2
Reset		Custom .....	6
Bayesian.....	7, 10	Enabled Network Tests checkbox .....	11
Reset .....	7	Group .....	6
Reset .....	10	IP4	
Reset Bayesian Database.....	10	Only .....	20
Reset DB.....	7	Recipients.....	21
Retain		Search .....	20
Days .....	7	SpamFilter Enabled .....	2
Retain .....	7	whitelist.....	15
Return		Select .....	2
Quarantine.....	18	Select .....	4
Return .....	18	Select .....	6
<b>S</b>		Select .....	11
Scan Images		Select .....	15
Check .....	2	Select .....	20
Scan Images.....	2	Select .....	21
Scanned		Select Bayesian Filter .....	7
Maximum Message Size .....	4	Select Blacklists .....	17
Scanned.....	4	Select Network Tests .....	11
Score .....	2, 12	Select Quarantine .....	20
Scores button.....	6	Select Settings .....	2
Search .....	20	Select Whitelists.....	15

Send email .....	21	SpamFilter	
Set		Configuring .....	2
Only From Trusted Networks.....	7	enabling.....	2
Set .....	4	SpamFilter.....	2
Set .....	7	SpamFilter.....	4
Settings button .....	21	SpamFilter.....	6
Show.....	20	SpamFilter.....	7
Simply.....	2	SpamFilter.....	10
SMTP Authentication .....	2	SpamFilter.....	11
Spam characteristics.....	15	SpamFilter.....	12
Spam Content.....	2	SpamFilter.....	15
Spam Level		SpamFilter.....	17
adjusting.....	2	SpamFilter.....	19
modify.....	2	SpamFilter.....	20
Spam Level.....	2	SpamFilter.....	21
Spam Level.....	4	SpamFilter Add-In	
Spam Quarantine		install .....	7
access .....	21	Outlook .....	7
configuring.....	21	SpamFilter Add-In .....	7
forwarded .....	21	SpamFilter Enabled	
Managing.....	20	Select .....	2
Spam Quarantine.....	2, 18, 19	SpamFilter Enabled.....	2
Spam Quarantine.....	20	SpamFilter menu.....	2, 7, 11, 12, 15, 17, 20
Spam Quarantine.....	21	SpamFilter Overview.....	1
Spam Quarantine Settings		SpamFilter Quarantine .....	20
access .....	21	SpamFilter Quarantine Settings .....	21
Spam Quarantine Settings.....	21	SpamFilter Settings	

## InstaGate SpamFilter

Quarantine.....	20	URL.....	20
SpamFilter Settings.....	4, 12	Use Extended Rules Enabled	
SpamFilter Settings.....	20	deselect .....	4
SpamFilter Test Scores		Use Extended Rules Enabled .....	4
Modifying.....	6	Use Historical Averaging	
SpamFilter Test Scores .....	6	Rate Individual Senders checkbox .....	4
SpamFilter's spam .....	4	Use Historical Averaging.....	4
Spammers.....	4, 11	User Quarantine Management.....	21
Subject.....	4, 18, 20	Users.....	21
<b>T</b>		<b>V</b>	
Teach		View Message	
Bayesian Filter.....	7	exit.....	18
Teach.....	7	View Message.....	18
ThreatWall.....	21	Viewing	
Threshold Settings .....	4	Messages .....	18
Training		Viewing .....	18
Bayesian.....	7	<b>W</b>	
Bayesian Filtering.....	7	Whitelists	
Training.....	7	Adding .....	19
Trusted Networks.....	2	Configuring .....	15
<b>U</b>		Whitelists.....	15
Unchecking Allow Client Authentication.....	2	Whitelists.....	19
Update Now		Wildcards .....	15, 17
clicking.....	4	<b>X</b>	
Update Now .....	4	X-Spam-Flag.....	2
URL		X-Spam-Report .....	4
following .....	20		

