
How to filter spam with Policy Patrol

Spam is offensive and annoying and decreases productivity and bandwidth. Policy Patrol offers numerous ways in which you can effectively filter and block spam messages. This document describes each method and provides the corresponding configuration instructions. With its powerful rules structure, Policy Patrol offers you the flexibility to decide which method(s) you wish to use, and allows you to customize each spam blocking method to fit your organization's specific needs.

Why use Policy Patrol to stop spam?

Policy Patrol offers a comprehensive and powerful set of features to help you put an end to unwanted mails, whilst keeping false positives at a minimum. Here are ten reasons why you should select Policy Patrol as your spam filtering solution:

1. Policy Patrol is an extremely comprehensive spam filter and combats spam on all fronts by using Bayesian filtering, checking for spam words, URLs, spam headers, sender domains, remote content, sender IP addresses, number of recipients, language character sets, illegal HTML and the absence of a plain text body part. False positives can be avoided by making use of (automatic) white lists.
2. **New:** Policy Patrol is the first Exchange add-on to support SURBL Lists, which are used to check URLs in the message body for known spammer domains.
3. Policy Patrol uses advanced keyword-filtering techniques with word pattern matching. By using regular expressions Policy Patrol can find many word variations with one single filter entry, such as `vi@gra`, `v*i*a*g*r*a` and `v|i|a|g|r|a`. Policy Patrol includes several sample filters with regular expressions, and also allows you to create your own filters.
4. Policy Patrol is one of the few products that can remove HTML tags before checking the email text. Therefore the product is capable of successfully stopping spammers who try to circumvent content filters by placing HTML comment tags within the text.
5. Policy Patrol can make use of multiple spam black lists and uniquely includes the possibility to take different actions for each list and each return. This is important since for instance open relay lists produce more false positives than known spammers lists and you would therefore need to take less 'drastic' action for messages from open relays. In addition to quarantining, Policy Patrol can reject (i.e. not download) spam messages that originate from IPs on real-time black lists, therefore saving bandwidth.
6. Policy Patrol includes recipient verification, which can be used to block NDR spam attacks and save bandwidth and storage space.

7. Policy Patrol can quarantine, add a tag or header or delete spam messages (with the possibility to undelete). By adding a header to spam messages, you can set up a rule in Outlook that places these messages in a 'Spam' folder for the user to review. Alternatively spam messages can be forwarded to a public folder.
8. Policy Patrol offers full integration with Exchange Server 2003 and Outlook 2003, by allowing you to apply a Spam Confidence Level to a spam message, which can then be placed in the user's junk folder.
9. Policy Patrol displays the conditions that triggered rule(s) including individual words and their score. This allows you to adjust your filters and conditions accordingly.
10. Policy Patrol blocks spam at server level, saving you the installation of spam filtering software on the client machines. With the many sample anti-spam rules, filters and templates, you can start blocking spam within minutes after installation.

What our customers say

'Policy Patrol has been in use for some time now and we think it is excellent! We catch over 1200 SPAM emails a day.'

Matt Franklin - Manager of Data Center Operations, RPM International Inc. (Medina, Ohio)

'Great product. Works better than any other SPAM filter we have tried. Clients are begging us for a SPAM solution.'

Ben Rutter - Project Coordinator, Lionfield Technology Solutions (Exton, Philadelphia)

'After looking into several e-mail filtering solutions, I decided to go with Policy Patrol because of its flexibility, ease of use and mail filtering effectiveness. Policy Patrol took no time to implement into our existing e-mail environment without any disruption to users. The Policy rules are very easy to setup, customisable and most important of all very effective in stamping out spam & virus infected e-mail, which was our number one priority.'

Owen Treanor - European MIS Coordinator, Rainbow Technologies (Surrey, UK)

'Great product, easy to configure, saves time & trouble. Policy Patrol has cut down on the SPAM & junk and made productivity go up. I'm able to spend time on things I want to do, instead of "Baby-sitting" the email server.'

Todd Munro - Network Administrator, LifeLink Tissue Bank (Tampa, Florida)

Quick Start

To quickly start blocking spam, enable the following sample rules in Rules > Sample Rules > Policy Patrol Spam Filter:

1. *Accept messages that exist in white lists* (enter email addresses and/or domains in the Newsletters filter and enter white listed words and phrases in

- the Company white list filter in Filters > Sample filters > Policy Patrol Spam Filter.)
2. *Automatic white list and Bayesian filter learning*
 3. *Quarantine messages from DNSBL and SURBL lists* (If Policy Patrol is not receiving messages directly from the Internet follow the instructions in the paragraph 'How to configure real time black lists (RBL)' - 'If Policy Patrol is not receiving mail directly from the Internet')
 4. *Quarantine non-legitimate messages* (you must first import approximately 2000 legitimate messages in the sample Bayesian filter, or wait until the Policy Patrol rule has automatically added them)
 5. *Quarantine spam messages*

By enabling these rules you will start blocking the majority of spam messages whilst avoiding false positives. Each Policy Patrol anti-spam feature is described in more detail in the paragraphs below.

How to configure Bayesian filtering

Bayesian filtering is used to calculate the probability that a message is non-legitimate by comparing the message content with two databases, one with legitimate mails and one with non-legitimate mails. The result is a probability score between 0 and 1, where 0 is a legitimate message and 1 is a non-legitimate message. Policy Patrol already includes a sample Bayesian filter that includes over 3000 non-legitimate messages. To start using Bayesian filtering, you need to enable the following sample rules:

- Automatic white list and Bayesian filter learning:** This rule automatically adds recipient email addresses of all outgoing emails (except for Delivery Status Notifications and out of office replies) to the 'Automatic white list'. In addition, it adds the messages (except for Delivery Status Notifications and out of office replies) to the Bayesian filter's legitimate database. After enabling the rule, you can simply wait for your Bayesian filter to fill up with legitimate messages (by default maximum is 5000).
- Quarantine non-legitimate messages:** This rule quarantines all externally received messages that have a Bayesian probability score of 0.8 or higher in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder. The Bayesian sample filter already includes over 3000 non-legitimate messages but you still need to add legitimate messages. You can automatically add legitimate messages to the filter by enabling the rule 'Automatic white list and Bayesian filter learning'. Alternatively, you can import messages into the Bayesian filter by going to **Bayesian filtering > Sample filter**, selecting **Bayesian filter** and clicking on **Import**. Select to import into the **Legitimate** database. You will be able to import messages from a mailbox or from a public folder. Note that it is better not to enable this rule until you have at least 2000 legitimate messages in the Bayesian filter.

How to configure real time black lists (RBL)

Real time black hole lists contain IP addresses of known spammers or open relays and are regularly updated. Policy Patrol can use these lists to identify messages as spam before they are actually downloaded. The accuracy of this type of filtering depends on the list you use. There are two types of lists:

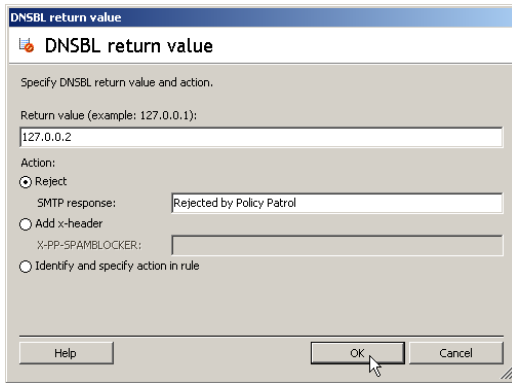
1. Lists of known spammer's domains, for example the [Spamhaus Block List \(SBL\)](http://spamhaus.org/sbl/) (<http://spamhaus.org/sbl/>)
2. Lists of mail servers that are open to relaying and therefore will allow spammers to send mail via their mail server. An example of this last kind of list is the [Open Relay Database \(ORDB\)](http://www.ordb.org) (<http://www.ordb.org>).

Whilst lists of the first type (spammer's domains) should be fairly accurate, lists of the second type, the open relay lists, can result in more false positives. This is because genuine persons that wish to contact your organization might not be aware that their mail server is being used for relaying. Therefore, Policy Patrol offers the possibility to handle messages differently for each spam list. For instance, you could reject all messages from domains listed on the Spamhaus Block List, and create a rule that quarantines or deletes mails from the Open Relay Database (for more information see paragraph 'What to do with messages flagged as spam').

To use real time spam black lists with Policy Patrol, you need to enable the following sample rules (If Policy Patrol is not receiving mail directly from the Internet, consult the paragraph below):

- Quarantine messages from DNSBL and SURBL lists:** This rule quarantines all externally received messages from senders on the SBL (www.spamhaus.org) or NJABL (www.dnsbl.njabl.org) real-time black lists, and messages that contain URLs from the SURBL list multi.surbl.org in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder.
- Add tag to messages on open relay list:** This rule adds the tag OPEN RELAY: to the subject of messages from senders on the ORDB list.

In the above rules, the spam messages are downloaded and then quarantined. However, you can also configure Policy Patrol to reject messages from senders on real-time black lists, saving the bandwidth needed to download the messages. To do this, go to **Spam blocker > Sample entries**. Select a list, for instance **SBL** and click **Properties**. Click on a return value and click **Properties**. Select **Reject** as the action and enter `Rejected by Policy Patrol` as the SMTP Response. Click **OK**. Repeat this for all return values. When you are done, click **OK**.



You can add more lists if you wish. You can also make a distinction between the returns of a list, by adding a separate entry for each list return. For instance, the DNSRBL list (www.dnsrbl.com) has several returns. If the DNSRBL list returns 127.0.0.4, the site has been identified as a constant source of spam. Therefore you would want to configure Policy Patrol to reject all messages that return this value. However, if the list returns the value 127.0.0.5 this indicates that the site is a smart host. Since this might create more false positives, you could select **Identify and specify action in rule** and then create a rule that adds a tag to the subject. For an overview of available spam black lists, go to <http://www.email-policy.com/Spam-black-lists.htm>.

If Policy Patrol is not receiving mail directly from the Internet

It is not possible to reject messages if Policy Patrol is not receiving messages directly from the Internet (for instance if installed behind a DMZ), since Spam blocker will resolve the IP address of the relay server and not the original sender of the mail. Therefore when configuring real-time black lists and IP ranges, you must select the option **Identify and specify action in rule** and select the rule condition **Spam blocker detected IP from DNSBL/IP range in headers**. When this option is selected Policy Patrol will check all message headers for the IP address, not just the last sending IP.

Testing Spam blocker

Some DNS blacklists offer a service that can test whether the mail server is configured correctly to block senders that are listed on the DNS Blacklist. For these tests to be successful the following conditions must be met:

1. The test mail must be sent from a mailbox on a mail server with Policy Patrol installed.
2. The machine on which Policy Patrol is installed must receive mail directly from the Internet.
3. In **Spam blocker** > <folder> > <spam list> > **Properties** > **Return value** > **Properties** the option **Reject** must be selected. This is because if Policy Patrol downloads the message, the service will think that the message was not detected by Policy Patrol.

To test ordb.org:

- Go to **Spam blocker** > <folder> > **ORDB** > **Properties** > **Return value** > **Properties**. Make sure that the option **Reject** is selected (you can enter any response, such as 'Rejected by Policy Patrol').
- Send a mail to ask-test-ordb@null.dk.
- You should get a mail back with the results of the test.

To test spamhaus.org:

- Go to **Spam blocker** > <folder> > **SBL** > **Properties** > **Return value** > **Properties**. Make sure that the option **Reject** is selected for all return values (you can enter any response, such as 'Rejected by Policy Patrol').
- Send a mail to nelson-sbl-test@crynwr.com.
- You should get a mail back with the results of the test.

How to configure Spam URL Realtime Block Lists (SURBL)

As opposed to RBL lists that include sender IP addresses and domains, SURBL lists are used to check URLs contained in the body of email messages. Even if spammers try to bypass existing heuristic and Bayesian filters by replacing text with images or including minimal text, they will still need to include a URL to be contacted on. Therefore checking the URLs against a list of known spammer domains provides an important additional layer of protection and can be successful where other filtering methods fail. SURBL lists require zero administration, are constantly updated and most of them are free to use. SURBL Lists also provide specific protection against the growing problem of phishing since they include domains of known phishing sources. To use SURBL lists with Policy Patrol, you need to enable the following sample rule:

- Quarantine messages from DNSBL and SURBL lists:** This rule quarantines all externally received messages from senders on the SBL (www.spamhaus.org) or NJABL (www.dnsbl.njabl.org) real-time black lists, and messages that contain URLs from the SURBL list multi.surbl.org in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder.

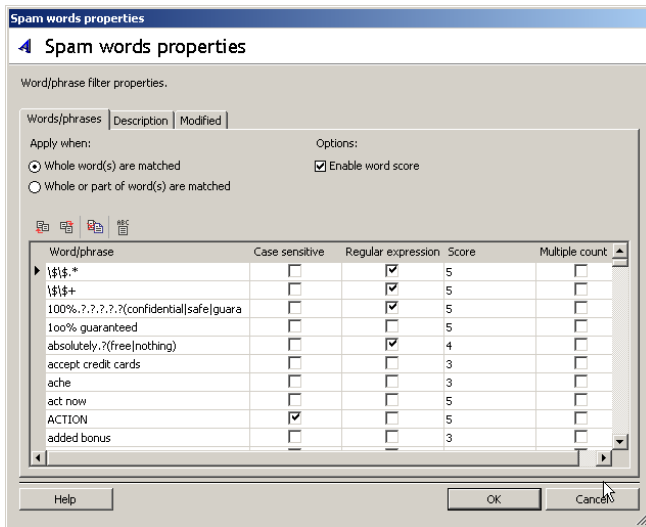
How to check for spam characteristics

Policy Patrol can also identify a large percentage of spam messages by checking for spam characteristics such as message content, spam headers, number of recipients, character set used and the absence of a plain text body part.

▪ Spam words in subject or body

Many spam messages can be identified by their message content. Words such as CLICK HERE, ACT NOW and the use of lots of exclamation marks clearly indicate spam. By using a word weighting system, indicating case sensitivity per individual word and using regular expressions, it is possible to accurately identify unwanted messages. False positives can be kept to a minimum by using negative as well as positive word scores. Since Policy Patrol removes all HTML tags before checking the

email text, the product is capable of successfully stopping spammers who try to circumvent content filters by placing HTML comment tags within the text. Policy Patrol can also be configured to specifically check the HTML code, which can be useful for checking links and/or scripts.



Policy Patrol includes a sample 'Spam words' and 'Offensive words' filter with commonly found spam words and phrases. To start checking for spam words, enable the following rule:

- Quarantine spam messages:** This rule quarantines all externally received messages that have spam words in the subject or body, match spam characteristics, or have a Spam Confidence Level of 7 or higher. The rule quarantines the messages in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder.

For more information on how to configure word/phrase filtering and regular expressions in Policy Patrol see the paragraph 'More information' at the end of this document.

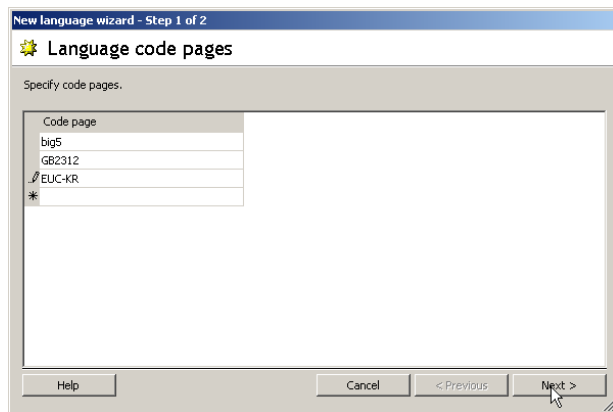
▪ **Commonly found spam characteristics**

Spam messages usually have the same 'tell tale' characteristics that can be used to identify and block these messages. By analyzing thousands of spam messages, Red Earth Software has been able to identify the most commonly found spam headers and has included them in the spam characteristics list. To check for these spam characteristics, you must select the rule condition **Message has spam characteristics**. You can also enable the sample rule **Quarantine spam messages** that checks for this condition.

- **Number of recipients**

Some spam messages are sent by including many addresses in the To: and Cc: fields. Policy Patrol allows you to check the number of recipients in order to filter out unwanted spam mails. To check for the number of recipients, you must select the rule condition **Message contains number of recipients**.

- **Language**



An increasing number of spam messages are originating from countries such as Korea or China. These messages arrive garbled since by default email clients cannot display the characters of these languages. To block messages that use certain character sets, you must first configure the language(s) you want to block from **Rules > General options > Languages**. Click **New**. Enter the character sets, for instance `GB2312` (Simplified Chinese), `big5` (Traditional Chinese), and `EUC-KR` (Korean). Click **Next** and enter a language name, for instance 'Chinese and Korean'. Click **Finish**.

Now select the rule condition **Message is of language**. Click on the link in the description and select the language you just created. You can also block all messages that do not use the English character sets. To do this you can create a rule that applies to all users and checks externally received messages. Do not enter any conditions. In exceptions select **Message is of language**. Click on the link in the description and select **English**. Select **Move to folder** in actions and select the quarantine folder. Now all messages that do not use one of the English character sets will be quarantined.

- **Absence of plain text body part**

HTML messages usually include a plain text version of the email so that recipients with email clients that cannot read HTML can still view the message in plain text. However, many spammers tend to send HTML messages without this plain text body part, not only to save on size but also to force recipients to read the HTML version. This enables spammers to embed an image link in the HTML code that connects to a site when the message is opened. In this way, spammers know how many people

have viewed their message. Furthermore by using a unique ID, spammers know exactly which recipients viewed the message and which email addresses are still 'live'. As soon as spammers know that an email address is live, they will send even more spam messages. To start checking for the absence of a plain text body part, enable the sample rule **Quarantine HTML mails without a plain text body**.

Specifying exceptions such as white lists

By specifying exceptions to a rule, false positives can be minimized. For instance, you can configure white lists with email addresses that Policy Patrol must always allow to pass through the filter, such as allowed newsletters, email addresses that your users have sent mails to (see paragraph 'How to create an automatic white list') or domains of important customers. Apart from sender white lists, you can also specify other exceptions such as the existence of a certain word/phrase in the subject or body.

Newsletters white list:

Policy Patrol includes a sample 'Newsletters' filter. You must add the email addresses or domains of your allowed newsletters to this filter. There are three ways to do this:

Edit the Newsletters filter:

1. Go to **Filters > Sample filters > Policy Patrol Spam Filter**. Double-click on the 'Newsletters' filter.
2. Enter the From: addresses of any allowed newsletters. You can either enter the email address or the domain (remember that the sending email address might change, although the domain is less likely to change). You can also use the * wildcard at the beginning or end of your entry. For instance, if you enter `*company.com`, the filter will include 'email.company.com' and 'testcompany.com'. If you enter `company.*`, this will include 'company.com' and 'company.co.uk'. When you are done, click **OK**.

Add to the filter from messages on hold:

1. Go to **Monitoring** and select the appropriate folder.
2. Right-click the message in question, choose **Add Sender to filter** and select the 'Newsletters' filter from the list. The From: email address of the quarantined message will now be added to the selected filter. This option is particularly useful if a genuine newsletter has been quarantined by mistake and you wish to add the Sender's address as an exception to the Spam blocking rule(s).

Add to the filter from History:

1. Go to **History**.
2. Right-click the message in question, choose **Add Sender to filter** and select the 'Newsletters' filter from the list. The From: email address of the message will now be added to the selected filter.

Company word/phrase white list:

Policy Patrol includes a sample Company white list filter. You can add words to this filter that can only be included in legitimate emails, such as your company name, your product name and your service name. To add to this filter, go to **Filters > Word/phrases**. Double-click on **Company white list** and add company specific words and phrases to the list.

Specifying exclusions in a rule:

To exclude a domain/email address white list from a rule, in step 4 of the Rules Wizard (Exceptions) select **Sender email/domain exists in filter**. Click on the **filter** link in the description and select the white list(s) from the list. To exclude a word/phrase white list from a rule, in step 4 of the Rules Wizard (Exceptions) select **Subject contains word/phrase**. Click on the link in the description and select the **Company white list**. Now go to 'Body' and select **Body contains word/phrase**. Click on the link and select the **Company white list** from the filter list.

How to block spammers that send from local domains

To stop spammers pretending to send internal messages and therefore bypassing rules that are applied to external messages, go to **<server name> > Advanced > System parameters**. Enter `MP_VERIFY_SENDER_LOCAL_IP_ADDRESS` as the name and set it to 1. Policy Patrol will now identify all messages that are sent from the local machine and are addressed to and from a local domain, as internal. If you have multiple mail servers or you have installed Policy Patrol on a separate machine you must add the IP addresses of the mail server(s) in the Local domains list in **<server name> > Advanced > System configuration > Local domains** tab. If you do not enter the IP addresses, all emails sent from these mail servers will be classified as external mails since they are not sent from the local machine.

How to stop NDR spam attacks

An NDR (Non Delivery Report) spam attack is when a spammer sends a large number of mails to a fake email address at your company with the intended spam victim as the sender. The result is that your mail server will send a non-deliverable report to the sender, i.e. the spam victim, with the original spam message attached.

With recipient verification enabled, Policy Patrol will simply reject these messages (i.e. not download them) and send an invalid address response to the sending mail server, saving valuable bandwidth and storage space. Legitimate emails that have been mistakenly addressed will still generate an NDR, however this NDR will not be sent by your mail server but by the sender's own mail server.

To configure recipient verification follow the next steps:

1. Go to **Spam blocker > Options > Recipient verification settings**.

2. Tick **Enable recipient verification** and select the domain controller. You can either use the default domain controller or select a different domain controller.
3. Select the Active Directory search root that must be used to verify recipients. Note that all your users must be in this Active Directory search root (in the same domain). If not all users are in the search root, mails to these users will be rejected.
4. Specify the SMTP response that must be given when a message contains a recipient that is not found in the Active Directory search root. If you enter 501 5.5.4 Invalid Address an NDR will be generated by the sending mail server. When you are done, click **OK**.

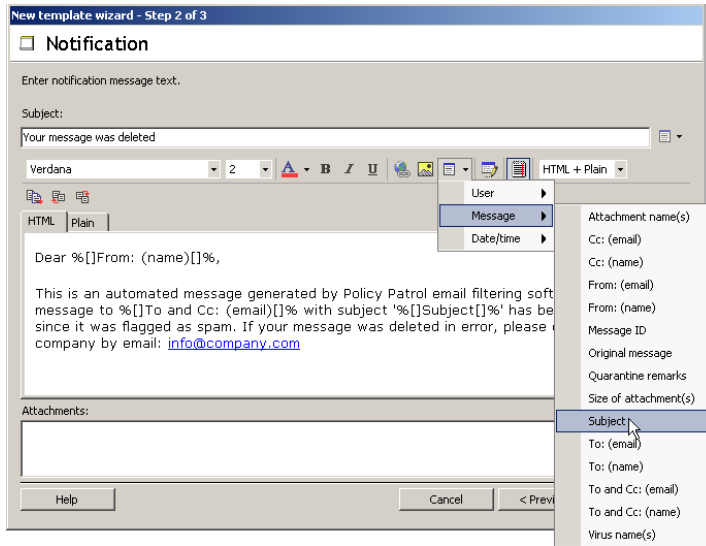
Important: Make sure that if Policy Patrol is not installed on the mail server machine or you have multiple mail servers sending outgoing email via the Policy Patrol installation, you enter the IP addresses of these mail servers in the Local domains list in **<server name> > Advanced > System configuration > Local domains**. This means that Policy Patrol will not apply the recipient verification to emails sent from these IP addresses. If you do not enter the IP addresses in the local domains list, Policy Patrol will block all outgoing mail since it will be detected as externally received mail that is not addressed to a local recipient.

Instead of rejecting messages that are not addressed to valid recipients, you can also delete or quarantine externally sent non-deliverable messages by enabling the sample rule **Quarantine externally sent NDRs** in Rules > Sample rules > Policy Patrol Enterprise.

How to configure a notification

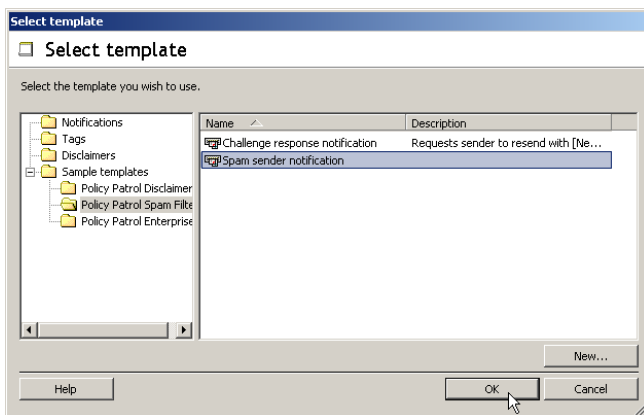
When a message is flagged as spam, you might want to send a notification to the sender, informing them that their message has been identified as spam and asking them to resend the message if it was wrongly detected as spam. To do this, create a notification template by following the next steps:

1. Go to Templates > Notifications. Click **New**. Select **Notification Template**. Click **Next**.

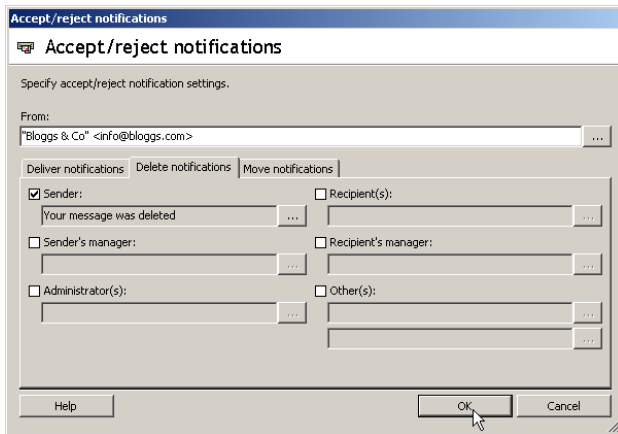


2. Enter a subject, for instance `Your message was deleted`, and enter your text in the HTML tab. For instance: `Dear %[]From: (name)[]%, This is an automated message generated by Policy Patrol email filtering software. Your message to %[]To and Cc: (email)[]% with subject '%[]Subject[]%' has been deleted since it was flagged as spam. If your message was deleted in error, please contact our company by email: info@company.com. You can insert more fields by clicking Insert field. If you wish to make changes in the HTML source, click on the View HTML Source button. Click on the Copy to.. button to copy the text from the HTML tab to the Plain tab. Click Next.`
3. Enter the Template name and click **Finish**.

Now you must configure your spam filtering rule(s) to send this notification message each time the rule triggers: In step 5 of the Rules Wizard (Actions), tick the secondary action **Send notification** and click on the **email notification** link in the description. Enter the From: address. If you wish to use a display name, enter the address as follows: "Display name" <email address>, e.g. "Company name" <info@company.com>. Tick **Sender** and select your template from the list.



You can also configure notifications to be sent when a quarantined message is delivered, deleted or moved. These notifications can be configured after you select **Move to folder** in step 5 of the Rules Wizard (Actions). Click on the **folder** link, and click on the **Notifications** button.



How to create an automatic white list

A number of false positives can be avoided by automatically creating a white list of email addresses that your users send messages to, and excluding this list from your spam filtering policies. In this way, you will not block any mails from existing customers and contacts. Note that it is important that this white list does not include recipients of NDRs and out of office replies, since in this case you might be adding spammers to your white list. To use the automatic white list:

1. Enable the sample rule **Automatic white list and Bayesian filter learning**. This will add the recipients of all outgoing mails (apart from delivery status notifications and out of office auto replies) to your white list.
2. You can either configure the Automatic white list as an exception in all your rules (in step 4 of the Rules Wizard (Exceptions) check **Sender email/domain exists in filter**), or you can create a rule that accepts all white listed messages and lets these bypass the spam filtering rules by unchecking the box **Process following rule(s)** in step 6 of the Rules Wizard (Name and Description). The latter method is used by the sample rule **Accept messages that exist in white lists**. It is important that this rule is ordered above the spam filtering rules in **Rules > Rule ordering**, and that any rules that must still be applied are ordered above this rule.

How to block mails that do not originate from the Automatic white list

Optionally, you can quarantine or delete all messages that do not originate from the Automatic white list. The drawback of blocking all mails that do not originate from the Automatic white list, is that any emails from new customers will always be blocked first. To block mails that do not originate from the Automatic white list:

1. Go to **Rules > <folder> > New**.

2. Select 'All users'. Click **Next**.
3. Select 'Only the following messages' and tick **Externally received**. Click **Next**.
4. Select 'No conditions'. Click **Next**.
5. Select 'Do not trigger rule if following exceptions are met'. In Headers, tick **Sender email/domain exists in filter**. Click on the **filter** link in the description. Select 'Automatic white list' and click **OK**. Click **Next**.
6. Select **Move message to folder**, select the quarantine folder and configure any secondary actions as required. For instance, you can configure a notification message to be sent to the sender and/or recipient (see below). When you are ready, click **Next**.
7. Do not schedule the rule and click **Next**.
8. Enter a name for the rule and click **Finish**.

How to require the sender to resend the message with a preset code

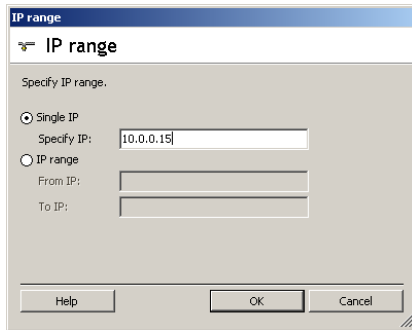
You can also send a notification message to the sender informing them that they must resend their message with a preset code in the subject so that their message will be allowed to pass through the filter. Upon receipt, Policy Patrol can remove the code from the subject. To configure the challenge/response system, enable the following rule(s):

- Block all messages not on automatic white list:** This rule blocks all messages from senders that are not listed on the 'Automatic white list' and sends a notification message to the sender requesting the sender to resend the message with [New customer] in the subject. Use this rule with caution since by enabling this rule you will block mails from all new customers and contacts. Remember to enter your company name in the 'Challenge response notification' template.
- Accept messages with [New customer] in subject:** This rule accepts all messages with the code [New customer] in the subject and adds the sender to the Automatic white list.
- Remove [New customer] from subject:** Enable this rule to remove the [New customer] code from the subject before the message is delivered to the recipient.

How to block IP addresses

Policy Patrol allows you to block single IP addresses and IP address ranges. To block IP addresses, follow the next steps:

1. Go to **Spam blocker > IP addresses** and click on **New**. The wizard will start up.
2. Select **IP range** and click **Next**.
3. Click **Add**. If you wish to block a single IP address, enter the IP address in **Single IP**. To block a range, select **IP range** and enter the start and end IP address. The entered addresses and all addresses in between will be included in the range. Click **OK**.



4. If you wish to reject messages: Select **Reject**. The message will not be downloaded by your mail server and will therefore not use up any bandwidth. The response you enter will be sent to the sending mail server. When you are ready, click **Next**. **Note:** You cannot select this option if Policy Patrol is installed behind a DMZ or not receiving mail directly from the Internet, since Spam blocker will resolve the IP address of the relay server and not the original sender of the mail. In this case you must select the option **Identify and specify action in rule** and select the rule condition **Spam blocker detected IP from DNSBL/IP range in headers**. When this option is selected Policy Patrol will check all message headers for the IP address, not just the last sending IP.

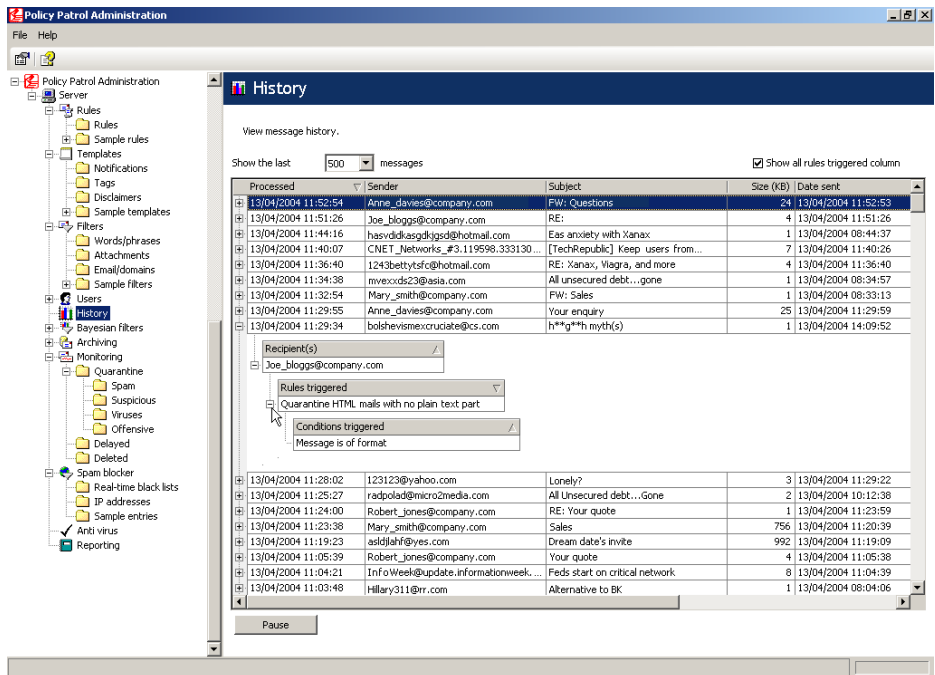
If you wish to download and process messages: Select **Identify and specify action in rule**. Now you must specify what action(s) Policy Patrol should perform by creating a rule that checks for the condition **Spam blocker detected IP/URL from DNSBL/SURBL/IP range** (if Policy Patrol is not receiving mail directly from the Internet you must select the option **Spam blocker detected IP from DNSBL/IP range in headers**). When you are ready, click **Next**.

5. Enter a name and description. If you do not want to check further DNSBL/SURBL/IP ranges if this IP range triggers, untick the option **Process next DNSBL/SURBL/IP range**. When you are ready, click **Finish**.

Checking why rules triggered

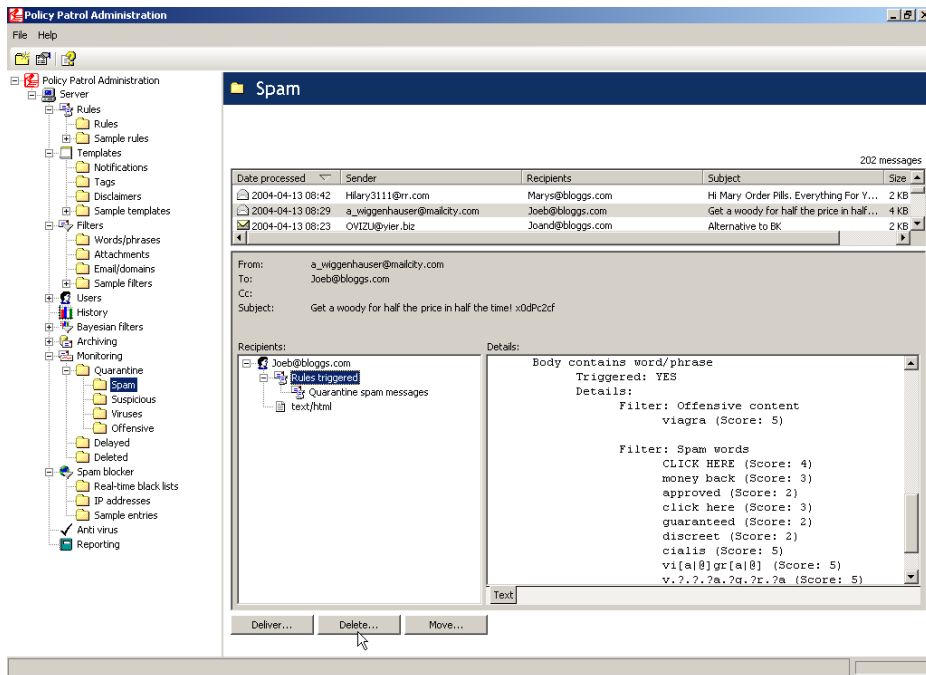
To help you check the accuracy of your rules, Policy Patrol provides detailed information on rules and conditions that triggered for each message:

1. Go to **History** and select the appropriate message.
2. Click on the plus sign next to the message. You will now see a list of recipients of the message. Click on the plus sign next to the recipient. Any triggered rule(s) will be listed. To view the conditions that were met for the particular rule, click on the plus sign next to the rule.



For quarantined messages you can also view this information in Monitoring:

1. Go to **Monitoring** and select the appropriate folder.
2. Select the relevant message in the top pane. The details of the quarantined message will be displayed in the bottom pane.
3. Click on **Rules triggered**. A report will be displayed giving details of each condition that was checked. If the rule was triggered by the presence of words, Policy Patrol will display each word found, including the corresponding word score.



What to do with messages flagged as spam

Policy Patrol offers several options for handling spam. The options (apart from rejecting messages which is done from the Spam blocker) can be configured in step 5 of the Rules Wizard (Actions). Each option is described below:

Reject messages

Policy Patrol allows you to reject (i.e. not download) messages from a certain IP address/IP address range or from an IP address listed on a real time black list (configured from the Spam blocker). Rejected messages do not use any bandwidth. However, rejected messages can no longer be retrieved.

Delete messages

Policy Patrol also provides the option to delete messages, with the possibility to undelete. To do this, select **Move message to folder** in step 5 of the Rules Wizard (Actions), and select the **Deleted** folder. The message will use bandwidth since the message is still downloaded. However, in case the message was deleted in error, the message can be restored and delivered. Automatic folder tasks can be configured to automatically (permanently) delete messages after a specified number of days.

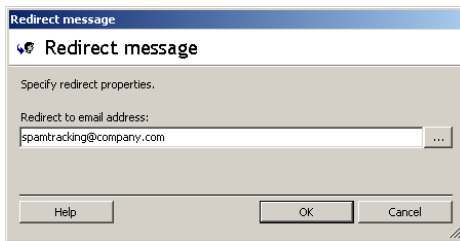
Quarantine messages

Policy Patrol can quarantine messages, i.e. place spam messages on hold on the server. To do this, select **Move message to folder** in step 5 of the Rules Wizard (Actions), and select the appropriate folder. Optionally a notification message can be sent when the message is quarantined, deleted or delivered. An Administrator or manager can then review the message and decide to deliver, delete or move the

message to another folder. Automatic folder tasks can be configured to move messages after a specified number of days and optionally send an email notification.

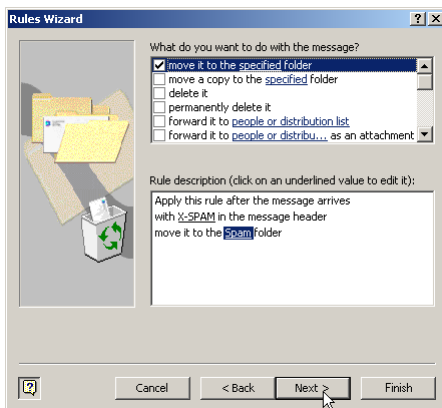
Redirect to a public folder

You can also configure Policy Patrol to forward suspected spam messages to a public folder, where they can be reviewed by several users. To do this, in step 5 of the Rules Wizard (Actions), select **Redirect** and enter or select the public folder to redirect the message to.



Add a header and place in Outlook folder

If you wish users to be able to review their own spam mails, you can configure Policy Patrol to add a header to the suspected spam message (in step 5 of the Rules Wizard (Actions) expand Modify message and select **Add X-header** as the secondary action). You can then set up a rule in Microsoft Outlook (Tools > Rules Wizard) that automatically places all messages with this header in a separate 'Spam' folder, enabling the user to review their own spam messages and decide whether they should be deleted.



Notifications

Policy Patrol can send notifications to the sender, recipient, Administrator, and sender's/recipient's manager. The notification message can include a number of fields, including the subject, original message text, and the sender and recipient email address. For more information on notifications consult the paragraph 'How to configure a notification'.

Add a tag to the subject

You can flag messages as suspected spam by adding a tag, such as 'SPAM:' to the subject. This will help users quickly identify possible spam mails when browsing through their emails.

Add sender to filter

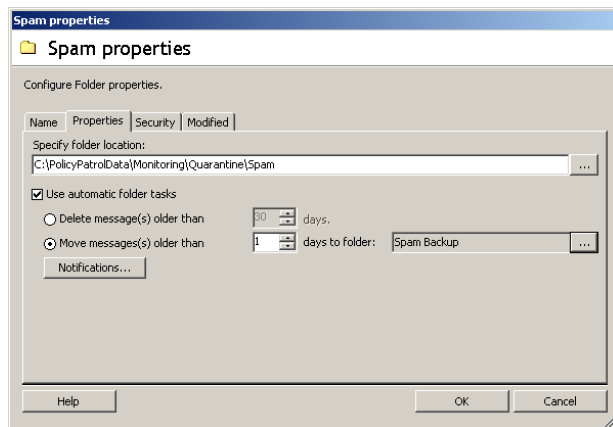
Policy Patrol can automatically add the sending domain or email address to a filter. For instance when a spam mail is received, you can add the sender email address to a black list by selecting the secondary action **Add sender address to filter**. The sample rule 'Quarantine spam messages' adds senders of suspected spam messages to the filter 'Spam senders'. Messages that are sent from email addresses on this black list (with the exception of white lists) are deleted by the sample rule 'Delete messages from known spam senders'.

Set Spam Confidence Level (SCL)

If you have Exchange 2003 you can configure Policy Patrol to add an SCL value that can be used by Outlook 2003 for placing the message in the user's junk mail folder. The SCL value can be from 0-9, with 0 indicating a legitimate message and 9 indicating a spam message. The value -1 indicates that the message is on a white list and must be let through. To add an SCL value to the message, select the secondary action **Set Spam Confidence Level (SCL)** and indicate the value to be assigned.

Workflow options

By making use of automatic folder tasks you can automatically delegate monitoring tasks to other users. For instance you can quarantine new spam messages in the 'Spam' folder that is monitored by the Administrator. If the Administrator was not able to check the message within 24 hours, the spam message will automatically be moved to the 'Spam Backup' folder, which is then reviewed by another member of staff. To configure automatic folder tasks, select the monitoring folder, right-click and choose **Folder properties**.



Go to the **Properties** tab and check the option **Use automatic folder tasks**. You can choose to delete or move messages older than a certain number of days. If you wish to send a notification each time a message is moved (or deleted) click on the **Notifications** button.

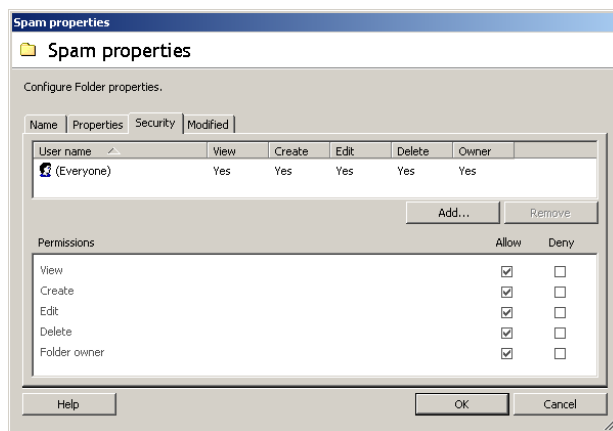
Take different actions according to certainty

Because of the product's flexibility, Policy Patrol allows you to create several rules that flag messages as spam with decreasing certainty. Then you can configure each consecutive rule to take less drastic action. For instance you could configure the following rules:

1. Reject mails originating from a sender on a real time black list, for instance Spamhaus block list.
2. Delete messages that include a URL on an SURBL list or produce a high total score of spam words, for instance a total score of 20 with the sample spam words filter.
3. Quarantine mails that contain spam characteristics or produce a total word score of 5 or higher.
4. Add a tag or header to messages originating from a sender on an open relay list.

User permissions

Policy Patrol includes powerful user permissions that allow you to offload tasks such as monitoring emails and updating white lists and black lists. Policy Patrol applies user permissions at three different levels: user access rights, component rights and folder rights. Component and folder rights are applied by specifying **View, Create, Edit, Delete** and **Folder owner** permissions. For more information on how to configure permissions, please consult the Policy Patrol product manual.



More information

- ⇒ For more information on how to configure Policy Patrol, please consult the program help or download the product manual from:
<http://www.policypatrol.com/docs/policypatrol3manual.pdf>.
- ⇒ For more information on how to configure word/phrase filtering in Policy Patrol, please download the document 'Word/phrase filtering with Policy Patrol' from:
<http://www.policypatrol.com/docs/PP3-WordFiltering.pdf>.

- ⇒ For more information on how to use regular expressions, please download the document 'Using regular expressions in Policy Patrol' from: <http://www.policypatrol.com/docs/PP3-RegularExpressions.pdf>.
- ⇒ If you still have questions after reading this document, please consult our online knowledge base at <http://www.redearthsoftware.com/kb.asp>, or send an email to support@redearthsoftware.com.

Contacting Red Earth Software

Red Earth Software LLC
200 Marcy Street
Portsmouth, NH 03801
United States
Phone: (603) 436-1319
Fax: (603) 457-8455
Sales: sales@redearthsoftware.com
Support: support@redearthsoftware.com

Red Earth Software (UK) Ltd
20 Market Place
Kingston-upon-Thames
Surrey KT1 1JP
United Kingdom
Tel: +44-(0)20-8605 9074
Fax: +44-(0)20-8605 9075
Sales: sales@redearthsoftware.co.uk
Support: support@redearthsoftware.co.uk

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2004 by Red Earth Software.