

This guide will help you start using Policy Patrol Spam Filter as quickly as possible. For more detailed instructions, consult the Policy Patrol manual.

Step 1. Prepare for installation

System requirements

Before installing Policy Patrol, check whether you meet the system requirements:

Policy Patrol Email (32-bit version):

- Windows Server 2003 or Windows 2000 Server/Advanced Server (or Windows XP Professional, Windows 2000 Professional or Windows Vista (apart from the Home edition) for installation on a separate machine)
- Exchange 2003, Exchange 2000, Exchange 5.5 (or Windows Small Business Server 2003/2000), Lotus Domino R5/6/7/8 or other mail server.
- Microsoft .NET Framework 2.0 (If you do not have this installed the Policy Patrol installation program will install it for you)

Policy Patrol Email for Exchange 2007 (64-bit version):

- Windows Server 2003 or Windows Server 2008 (64-bit).
- Microsoft Exchange Server 2007 or Windows Small Business Server 2008
- Microsoft .NET Framework 2.0 (If you do not have this installed the Policy Patrol installation program will install it for you)


Do I need the 32-bit version or the 64-bit version?

- If you do not have Exchange 2007, you need the 32-bit version.
- If you are installing Policy Patrol on Exchange 2007, you need the 64-bit version.
- If you have Exchange 2007 but are installing Policy Patrol on a separate machine, you need the 32-bit version.


⇒ If you have **Exchange 2007**, you must install Policy Patrol for Exchange 2007 (64 bit). Policy Patrol for Exchange 2007 can be installed on the following roles (there is no difference in functionality for either role):

- Edge Transport Role
- Hub Transport Role

If you are not installing Policy Patrol on the same machine as Exchange 2007, you must download the 32-bit version and follow the instructions for installing Policy Patrol on a separate machine:

 [Installing Policy Patrol on a separate machine](http://www.policypatrol.com/docs/PP6-SeparateMachine.pdf)
(<http://www.policypatrol.com/docs/PP6-SeparateMachine.pdf>)

⇒ If you have **Exchange 2000/Exchange 2003** you can install Policy Patrol on the Exchange server machine (recommended) or on a separate machine. If you are installing Policy Patrol on the same machine as Exchange, skip this section and proceed to 'Step 2. Install Policy Patrol'. If you install Policy Patrol on a non-Exchange Server machine, Policy Patrol will not process internal mails. Download the following document for instructions on how to install Policy Patrol on a separate machine:

 [Installing Policy Patrol on a separate machine](http://www.policypatrol.com/docs/PP6-SeparateMachine.pdf)
(<http://www.policypatrol.com/docs/PP6-SeparateMachine.pdf>)

⇒ If you have **Exchange 5.5**, you must install Policy Patrol on a separate Windows 2000/2003/XP machine and forward your mail to the Windows SMTP service on the Policy Patrol machine. Policy Patrol does not offer internal mail filtering for Exchange 5.5. Policy Patrol can retrieve your users & groups from Active Directory or Exchange 5.5. Download the following document for instructions on how to install Policy Patrol with Exchange 5.5:

 [Installing Policy Patrol with Exchange 5.5](http://www.policypatrol.com/docs/PP6-Exchange55.pdf)
(<http://www.policypatrol.com/docs/PP6-Exchange55.pdf>)

⇒ If you have **Lotus Domino R5/6/7/8 Mail Server** (or another mail server), you must install Policy Patrol on a separate Windows 2000/2003/XP machine. Policy Patrol does not offer internal mail filtering for Lotus Domino. Policy Patrol can retrieve Lotus Domino users & groups and their user properties for the user merge fields. Download the following document for instructions on how to install Policy Patrol with Lotus Domino:

 [Installing Policy Patrol with Lotus Domino](http://www.policypatrol.com/docs/PP6-LotusDomino.pdf)
(<http://www.policypatrol.com/docs/PP6-LotusDomino.pdf>)

⇒ Policy Patrol (32-bit and 64-bit) can be installed in a **clustered** environment. If you wish to install Policy Patrol 32-bit in an Active/Passive cluster, download the document below for further instructions (Policy Patrol 32-bit does not support Active/Active clusters):

 [Installing Policy Patrol in a cluster](http://www.policypatrol.com/docs/PP6-Clustering.pdf)
(<http://www.policypatrol.com/docs/PP6-Clustering.pdf>)

Note: You need to purchase an additional server license for the clustered node. The additional server license cost is found in the price list at <http://www.policypatrol.com/pricing.htm>.

⇒ If you have **frontend and backend** Exchange servers, you must always install Policy Patrol on the backend server. However if you use email clients that are using the frontend server to relay their email, you must install Policy Patrol on the frontend server as well as the backend server.

Note: You need to purchase an additional server license for each additional Policy Patrol server installation. The additional server license cost is found in the price list at <http://www.policypatrol.com/pricing.htm>.

⇒ If you have **Policy Patrol 4 or 5** installed, you can perform an upgrade to version 6 whilst keeping your existing configuration. For further instructions on this, please consult the following document:



[Policy Patrol 6 Upgrade Guide](http://www.policypatrol.com/docs/PP6-UpgradeGuide.pdf)

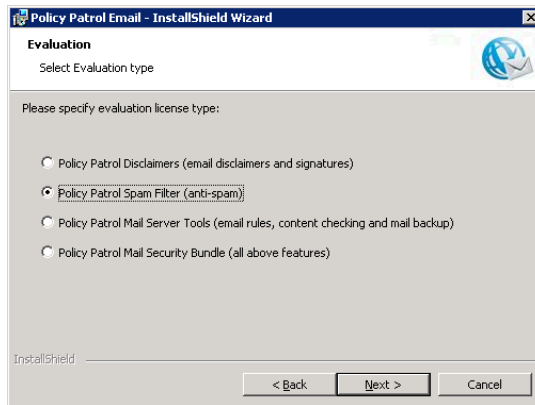
(<http://www.policypatrol.com/docs/PP6-UpgradeGuide.pdf>)

⇒ If you have **Policy Patrol 1, 2 or 3** installed, it is not possible to use your existing configuration files in version 6. To migrate your existing configuration to version 6, please consult our migration guide at <http://www.policypatrol.com/pp6migrationguide.htm> and follow the instructions on the page.

Step 2. Install Policy Patrol

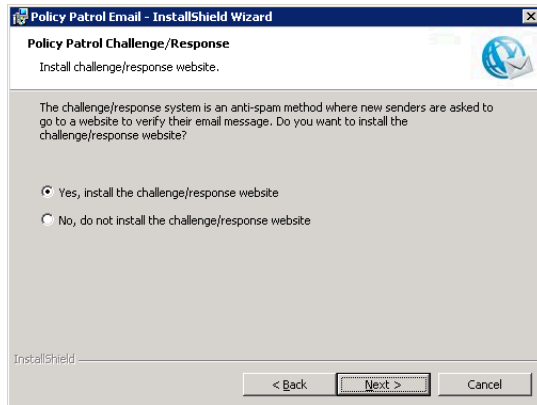
1. Double-click on **PolicyPatrol.exe** (32-bit version) or **PolicyPatrol2k7.exe** (64-bit version). The Install Program will start up. If you do not have Microsoft .NET Framework installed, the Policy Patrol installation program will download it for you.
2. In the Welcome screen, click **Next**.
3. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
4. Select the installation type. If you select **Complete**, the complete program will be installed. If you only wish to install the Administration console (for remote administration), select **Administration**.
5. Enter your user name, company name and Policy Patrol serial number. If you are evaluating Policy Patrol, leave the serial number field empty. Click **Next**.

6. **If you did not enter a serial number:** A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Spam Filter** and click **Next**.

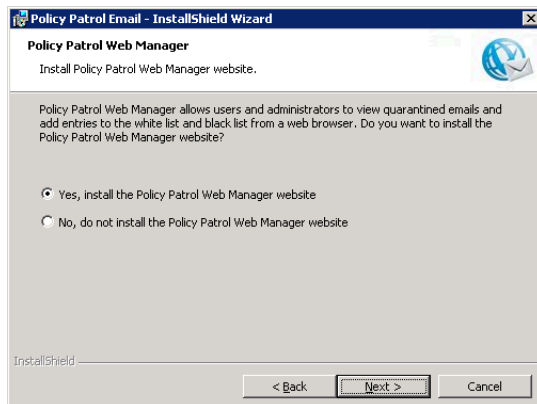


Note: If you are evaluating Policy Patrol and later wish to try out a different Policy Patrol edition you can go to **<server name> > Security > Licenses**, select the license and click **Remove**. Policy Patrol will warn that no valid license is found. Click **OK**. A dialog will now pop up allowing you to select a new evaluation license type.

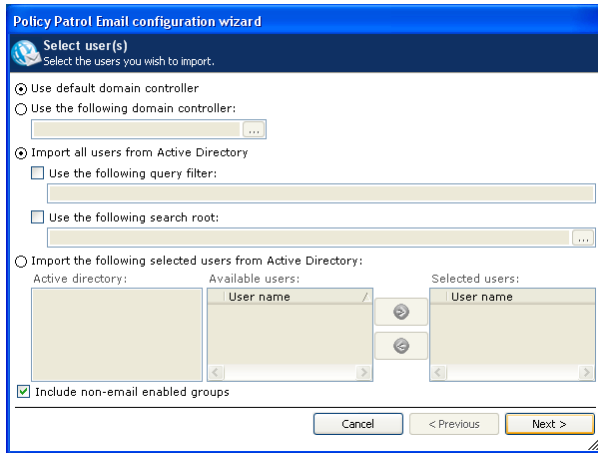
7. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email (32-bit version) or C:\Program Files\Red Earth Software\Policy Patrol Email for Exchange 2007 (64-bit version). If you wish to change the location, click **Change** and select another folder. When you are ready, click **Next**.
8. Specify the notification settings. Enter the From:, To:, Cc: and Bcc: fields for the Policy Patrol notification emails. Policy Patrol notification emails inform you about evaluation expiry dates, licensing issues and new updates to the program. The From: display name is pre-configured as Administrator, but you can change this by entering the following: "Display name" <email address>, i.e. "Joe Bloggs" <jbloggs@bloggsco.com>. Click **Next**.
9. Select whether you wish to install the challenge/response website. This website is needed if you wish to make use of the challenge/response system that asks new senders to go to a website and verify their email in order for the message to be delivered. Click **Next**.



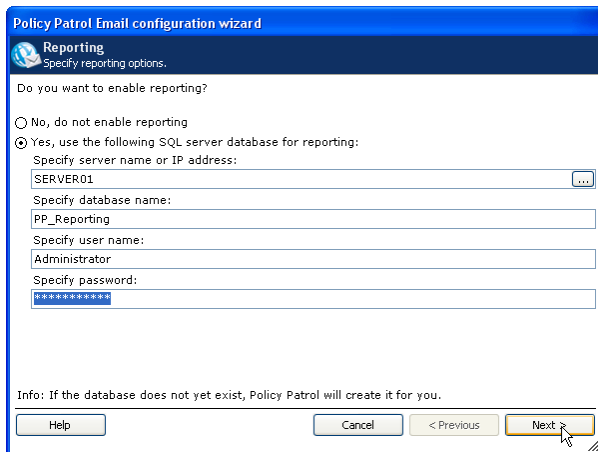
10. Select whether you wish to install the Policy Patrol Web Manager website. This website is needed if you wish to allow users and Administrators to view quarantined emails via a web browser (required for the quarantine report). Click **Next**.



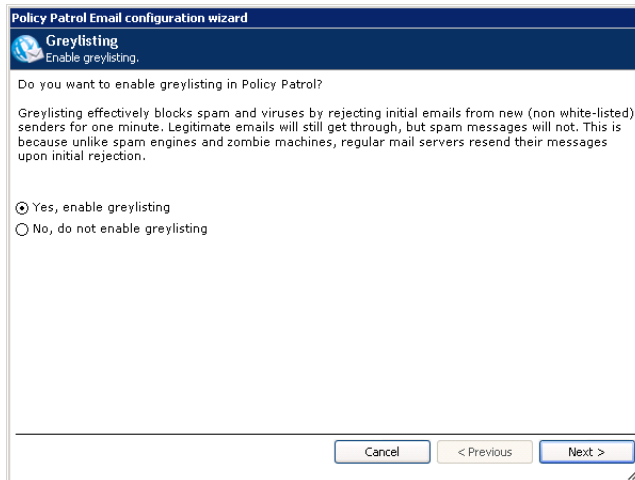
11. Click **Install** to start installing.
12. When the installation wizard has finished copying the files, click **Finish**.
13. The configuration wizard will now start up. Click **Next** in the Welcome screen.
14. Specify the location from where you would like to import your users (Active Directory, Exchange 5.5, Lotus Domino or Manual input). Click **Next**. (Note: the 64-bit version only includes the Active Directory and Manual Input options.)
15. Specify the server or domain controller and select the users that you wish to license. You can either license all users or you can select only certain users to be licensed. For more information on the different options, consult the product manual. Click **Next**.



16. Select whether you wish to enable reporting. If you enable reporting you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically create the database for you. If you do not have SQL Server, you can also specify an MSDE or SQL Server Express database. Click **Next** to continue.



17. Select whether you wish to enable greylisting. Greylisting effectively blocks spam and viruses by initially rejecting messages from new, non white-listed senders for one minute, therefore allowing legitimate emails through without any user intervention, and blocking the non-legitimate emails. Select whether you wish to enable greylisting, and click **Next**.



18. In the Configuration complete dialog, click **Finish**.




Step 3. Configure Anti-Spam

Policy Patrol will start blocking spam straight after installation with the default anti-spam configuration. However there are still a few things that you need to do in order to fine tune the spam filtering.

Default anti-spam configuration

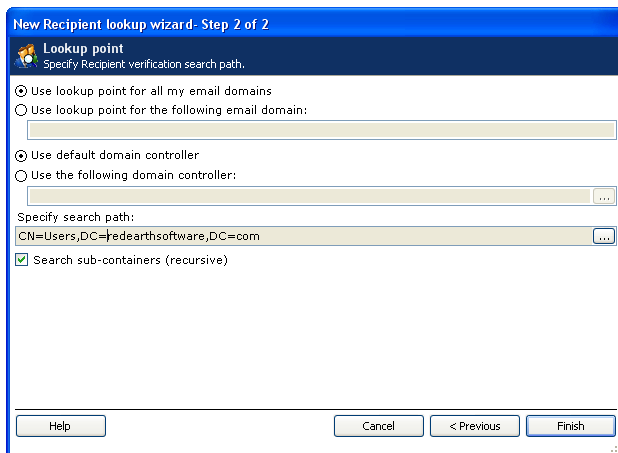
Policy Patrol Spam Filter is preconfigured to stop spam right out of the box using a number of spam blocking techniques including DNSBL lists, SURBL lists, Sender Policy Framework, heuristic filtering and header filtering. By default the program makes a distinction between **Known spam** and **Suspected spam**. The advantage of this is that it allows you to only focus on suspected spam messages and not waste time on known spam. Known spam is placed in the Known spam monitoring folder and is deleted after 7 days. Suspected spam is placed in the Suspected spam folder and is deleted after 15 days.

What you still need to do:

- **Add addresses to the Email white list:** By default, Policy Patrol automatically adds the recipients of any new outgoing emails to your Email white list. You can easily speed up the creation of your white list by importing email addresses from sources that already contain legitimate contacts for your company; recipients in Sent Items, Active Directory contacts and Outlook contacts. To do this, go to **Anti-spam > Black/white lists > Email/domain white list**. To import the recipients from the Sent Items folder in Outlook, click on the **Import from Sent Items**  icon in the toolbar. To import your Active Directory contacts into the white list, click on the **Import Active Directory contacts**  icon in the toolbar. To import Outlook contacts into the white list click on the **Import Outlook contacts** icon  in the toolbar.
- **Add words to the Word/Phrase white list:** Go to **Anti-spam > Black/white lists > Words/phrases white list**. Enter your company name and your product/service

names in the word/phrase white list so that emails containing these words in the body or subject will automatically be let through. Important: Remember to select the option **Whole words are matched**, and only enter words that are uniquely found in your legitimate messages.

- Configure Recipient Verification: Policy Patrol can reject messages without a valid recipient address, saving bandwidth and disk space. To reject messages that are not addressed to valid recipients, go to **Anti-spam > Address verification**. In **Recipient verification** tick the option **Drop SMTP connection when x number of invalid recipient(s) are detected**. By default the number is set to 2. When you select this option you will be asked to configure a recipient lookup point. Click **Yes** to configure a Recipient lookup point. Select the Lookup method (Active Directory, Exchange 5.5 or Other LDAP service (for Lotus Domino)). Click **Next**. In 'Specify search path', click on the ... button to browse to the path where your users reside. Click **Finish**. If you have more than one location where your users are kept, repeat this for every different lookup method you wish Policy Patrol to use.



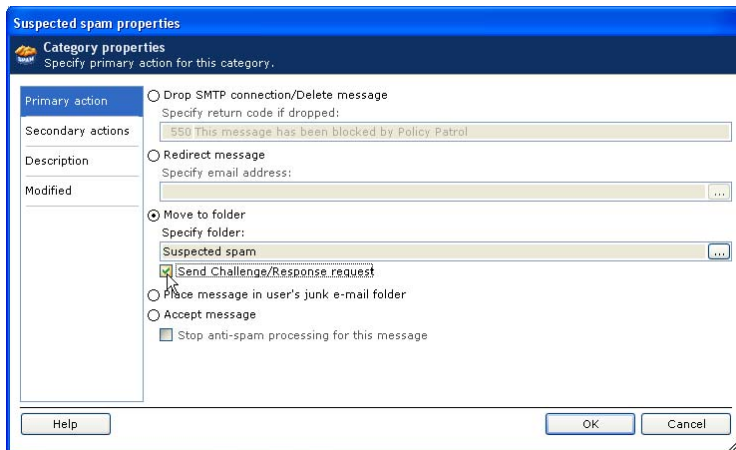
- Configure Greylisting: In case you did not enable greylisting during installation, it is highly recommended to enable this. Greylisting effectively blocks spam and viruses by initially rejecting messages from new, non white-listed senders for one minute, therefore allowing legitimate emails through without any user intervention, and blocking the non-legitimate emails. You can enable greylisting by going to **Anti-spam > Greylisting** and checking the box **Enable greylisting**.
- Configure Bayesian filtering: Before you enable Bayesian filtering, you should have at least 1000 spam messages and 1000 legitimate messages in the database. You can either import legitimate messages by using mails exported from Outlook or you can wait until the legitimate database is automatically filled with 1000 messages through the automatic learning feature. When there are 1000 messages in both the spam and legitimate database, Policy Patrol will automatically send an email notification to the Administrator, informing that Bayesian filtering can now be enabled. To enable Bayesian filtering, go to **Anti-spam > Bayesian filter** and select **Enable Bayesian filter spam protection**.

- **Select spam management method:** Users can receive a daily quarantine report with newly quarantined spam messages from where they can view, deliver and white list messages. To enable this report for all users, go to **Monitoring folders > Quarantine reports**. Right-click on the **Suspected spam report** and select **Enable** (for more information, see Step 4). It is also possible to forward all spam to the junk mail folder instead. For more information on how to configure this, please consult the product manual.

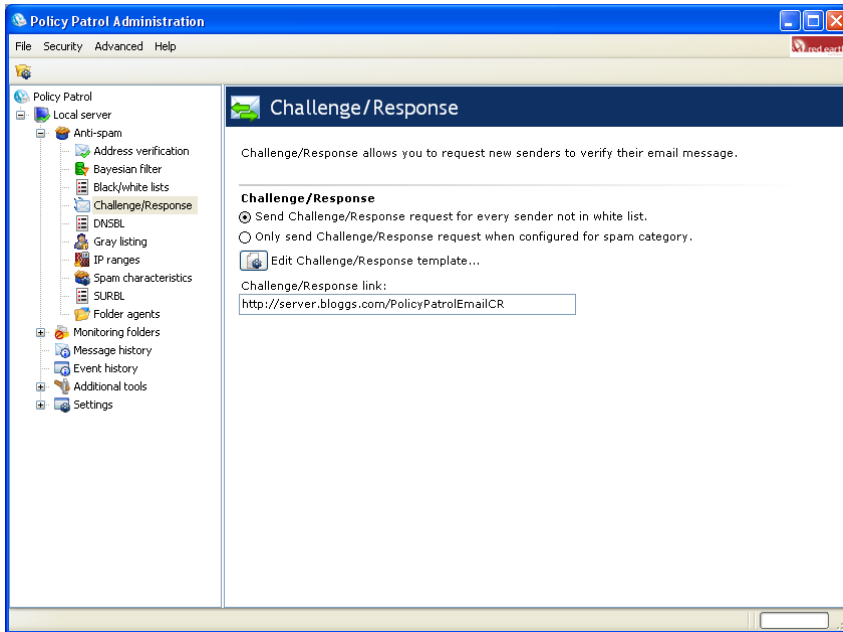
If you want to use Challenge/Response:

Challenge response is a system where new senders are asked to verify their message via a website. Until the message is verified, the message is quarantined in the Challenge/Response monitoring folder. As soon as the sender verifies their identity, the message is automatically delivered and the sender is added to the white list. If you want to send challenge/response replies to all or particular messages you can do so as follows:

Send challenge/response for spam messages only: If you only want to send challenge/response replies for those messages that Policy Patrol has flagged as spam, you must go to **Anti-spam**, select the appropriate Spam category and click **Edit**. In the Primary action tab, make sure that the action **Move to folder** is selected and tick the option **Send challenge/response request**. Repeat this for each spam category if applicable.



Send challenge/response for all messages not in white list: If you want to send a challenge/response reply to all new senders not in the white list, you must go to **Anti-spam > Challenge/Response** and select the option **Send Challenge/Response request for every sender not in white list**.




Policy Patrol includes more anti-spam features, such as country blocking, IP address blocking, verify MX record/SMTP connection, and Email/domain address black lists. For more information on how to configure these options, please consult the product manual.

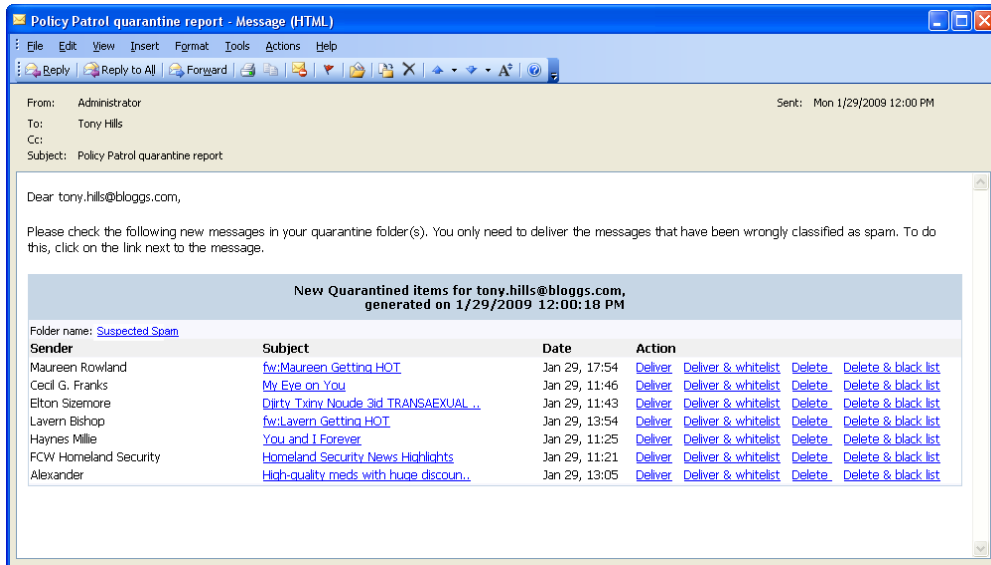
Step 4. Spam management

If you want your users to be able to manage their own spam you can configure a quarantine report to be sent to the users including newly quarantined items, and you can provide them with access to the Policy Patrol Web Manager:

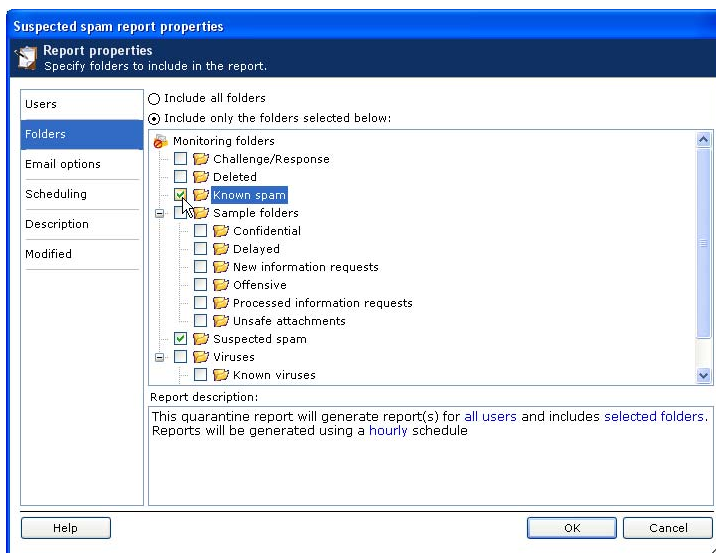
- **Web Manager:** The Policy Patrol Web Manager allows users to view their own quarantined spam messages via a web browser and add entries to the white list and black list. The Policy Patrol User Web Manager can be accessed from the following link: <http://IPaddress/PolicyPatrolEmail/WebManager.aspx> (where IP address is the IP address of the Policy Patrol machine). A Policy Patrol Web Manager user guide and a sample user memo that you can use to inform your users about the new spam management system are available for download from the following links:

 [Sample user memo](#)
(<http://www.policypatrol.com/docs/PP6-UserMemo.doc>)

 [Policy Patrol Web Manager User guide](#)
(<http://www.policypatrol.com/docs/PP6-UserGuide.doc>)



- Quarantine report (requires Web Manager):** Policy Patrol includes a sample quarantine report that sends a list of newly quarantined items in the Suspected spam folder once a day. To enable this report for all users, go to **Monitoring folders > Quarantine reports**. Right-click on the **Suspected spam report** and select **Enable**. To view the settings of the quarantine report, double-click on **Suspected spam report**. You will be able to change the users, folders to be included, email subject, message, frequency of the report etc. The preconfigured report only includes newly quarantined messages from the Suspected spam category (since messages classified within the Known spam category will usually not need to be checked). However if you also want to include the messages from the Known spam category in the report, select the **Folders** tab in the left column, check the box next to the **Known spam** folder and click **OK**.



It is also possible to forward your users' spam messages to the junk mail folder in Outlook so that they can view the messages from there. For more instructions on how to do this, please consult the product manual.

Step 5. Tracking

If you want more information on a quarantined message (for instance to find out why it was quarantined), go to the respective **Monitoring folder** (in the Policy Patrol Administration console) and select the message. The bottom pane will display the Message details. Click on the **Anti spam report** tab. This tab includes detailed information on the results of each spam filtering method and if relevant any words found and their score.

If you want more information on a particular message that was processed by Policy Patrol (but is not, or no longer in quarantine), you can go to the **Message history** node. Message history displays a list of the last 2000 messages processed by Policy Patrol. The list is continually updated and displays the date/time processed, sender, recipient(s), subject, size of the message, and the action that was taken. Select the message to view the message details in the bottom pane. Click on the **Anti spam report** tab. This tab includes detailed information on the results of each spam filtering method and if relevant any words found and their score.

The screenshot shows an Outlook email window with the following details:

- From:** "EEM Product Update Newsletter" <eemproductupdate@elec-p-media.com>
- To:** John Doe <john.doe@company.com>
- Subject:** Update on Cooling Products, fans, fan guards, heat sinks and more.
- Date sent:** 1/25/2007 9:30:00 ...
- Attachments:** multipart/alternative (text/plain, text/html)

The main content area displays the **Anti spam report** for the selected message:

Anti spam report	
Message origin	
Remote IP address	205.162.40.37
Remote domain	40.37.omessage.com
White listed	
Email address	No
Email address (Database lookup)	No
IP address	No
Words/phrases	No
Black listed	
IP address (sender)	No
IP address (headers)	No
Email address	No
Words/phrases	Yes
click: here	2
cool	3
r tes	3
unsubscribe	2
Total score (Threshold)	10 (5)
Sender Policy Framework	
Sender address	Passed
DNSBL	
SBL (205.162.40.37)	Not listed
DNSBL (205.162.40.37)	Not listed
ORDB (205.162.40.37)	Not listed
CBL (205.162.40.37)	Not listed

At the bottom of the report pane, there are navigation tabs: Plain text, Headers, Message details, **Anti spam report** (selected), and Anti virus report. Below the report pane are buttons for Deliver, Move, and Delete.

Policy Patrol also keeps a record of certain user actions, including delivering and deleting messages and adding addresses to the white list and black list. Each day a new Audit file is created in the \Program Files\Red Earth Software\Policy Patrol Email\AuditLog folder. The file is called PPE_AUDITyyyymmdd.log.

	A	B	C	D	E	F	G	H	I
1	Date	Time	Server	Client	User	Action	Result	Sender	Recipient
2	3/21/2007	4:50:52 PM	MLSRVR	CLIENT5	BLOGGS\Sarah.Jones	Delete	Success	dwamynavidm@amynvidavid.com	sarah.jones@bloggs.co
3	3/21/2007	4:51:20 PM	MLSRVR	CLIENT1	BLOGGS\Trevor.Whitely	Deliver	Success	subscriptions@sqlservercentral.c	trevor.whitely@bloggs.c
4	3/21/2007	5:29:43 PM	MLSRVR	CLIENT3	BLOGGS\Dawn.Peters	Deliver	Success	hcheng@enselearning.com	dawn.peters@bloggs.co
5	3/21/2007	5:29:50 PM	MLSRVR	CLIENT4	BLOGGS\John.Doe	Deliver	Success	bounce-1053-6824117@lyris.net	john.doe@bloggs.com
6	3/21/2007	5:29:59 PM	MLSRVR	CLIENT5	BLOGGS\Sarah.Jones	Deliver	Success	bounce-1051-6917761@lyris.net	sarah.jones@bloggs.co
7	3/21/2007	5:30:55 PM	MLSRVR	CLIENT6	BLOGGS\Sales	Deliver	Success	news@insideapple.apple.com	sales@bloggs.com
8	3/21/2007	5:31:26 PM	MLSRVR	CLIENT1	BLOGGS\Trevor.Whitely	Deliver	Success	info@emailkfc.com	trevor.whitely@bloggs.c
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									

Step 6. More information

⇒ Below is a list of the most frequently asked anti-spam questions:

1. I'm having problems enabling the junk mail folder
2. Spam filter is letting spam through
3. White listed messages are still being blocked
4. How can I configure user based anti-spam?
5. What can I do to minimize false positives?
6. How can I forward spam mails to the user's junk mail folder?

The answers to these questions and more can be found in our knowledge base at:
<http://www.policypatrol.com/kb.asp>

- ⇒ For more information on how to configure Policy Patrol, please download the product manual from:
<http://www.policypatrol.com/download.htm>.
- ⇒ If you have any technical or configuration questions please send an email to:
support@reearthsoftware.com.
- ⇒ If you require any assistance, please contact us at one of the following offices:

Red Earth Software, Inc.
 595 Millich Drive, Suite 210
 Campbell, CA 95008
 United States

Red Earth Software (UK) Ltd
 20 Market Place
 Kingston-upon-Thames
 Surrey KT1 1JP



Toll-free: 1-800-921-8215
Phone: (408) 370 9527
Fax: (408) 608 1958
Sales: sales@reearthsoftware.com
Support: support@reearthsoftware.com

United Kingdom
Tel: +44-(0)20-8328 9830
Fax: +44-(0)20-8711 5771
Sales: sales@reearthsoftware.co.uk
Support: support@reearthsoftware.co.uk

Red Earth Software Ltd
Sonic House, Suite 301
43 Artemidos Avenue
6025 Larnaca
Cyprus
Tel: +357-24 828515
Fax: +357-24-828516
Sales: sales@reearthsoftware.com
Support: support@reearthsoftware.com

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2009 by Red Earth Software.

