

Quick Start

Policy Patrol Spam Filter 4



This guide will help you start using Policy Patrol 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:

- Windows 2000 Professional/Server/Advanced Server, Windows Server 2003 or Windows XP Professional.
- Exchange 2003, Exchange 2000, Exchange 5.5, Lotus Domino R5/R6/R7 or other mail server.
- Microsoft .NET Framework 1.1 (If you do not have this installed the Policy Patrol installation program will download it for you)

⇒ 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/PP4-SeparateMachine.pdf)

(<http://www.policypatrol.com/docs/PP4-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/PP4-Exchange55.pdf)

(<http://www.policypatrol.com/docs/PP4-Exchange55.pdf>)

⇒ If you have **Lotus Domino R5/R6/R7 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/PP4-LotusDomino.pdf)
(<http://www.policypatrol.com/docs/PP4-LotusDomino.pdf>)

⇒ If you wish to install Policy Patrol in an **Active/Passive cluster**, download the document below for further instructions:

 [Installing Policy Patrol in a cluster](http://www.policypatrol.com/docs/PP4-Clustering.pdf)
(<http://www.policypatrol.com/docs/PP4-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 need to determine on which machine(s) you must install Policy Patrol according to the following guidelines:

- (1) If you use POP3 clients on the frontend server you must install Policy Patrol on the frontend server.
- (2) If you use Outlook, Outlook Web Access (connecting to the frontend or backend server), or POP3 clients connecting to the backend server you must install Policy Patrol on the backend server. Note: If you have the SMTP service installed on the frontend server and all outbound mails are relayed to the frontend server you can also only install Policy Patrol on the frontend server. However, this will mean that Policy Patrol will not process internal mails since these are routed internally on the backend server and will not pass through Policy Patrol.

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>.

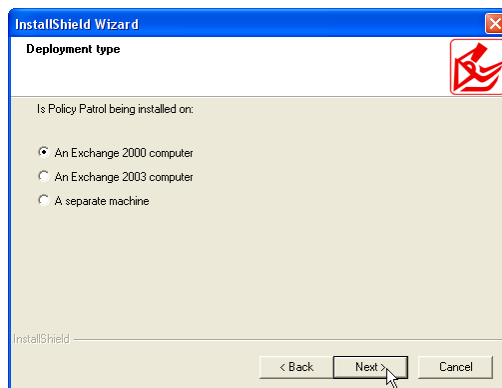
⇒ If you have **Policy Patrol 3.x** installed, you must uninstall Policy Patrol 3.x by going to Add/Remove programs. Since there have been many updates to the program, it is not possible to use your version 3 configuration files in version 4. To migrate your existing configuration to version 4, please consult our migration guide at <http://www.policypatrol.com/pp4migrationguide.htm> and follow the instructions on the page.

⇒ If you have **Policy Patrol 2.x** installed, you must uninstall Policy Patrol 2.x by going to Add/Remove programs. Since there have been many updates to the program, it is not possible to use your version 2 configuration files in version 4. To migrate to version 4, export your templates and filters and copy the descriptions of your rules. Import the templates and filters in version 4 and recreate the rules using your rule descriptions from version 2.

- ⇒ If you have **Policy Patrol 1.x** installed, you must uninstall version 1 before you install version 4. To do this, go to Start > Settings > Control Panel > **Add/Remove programs**. Select **Policy Patrol Disclaimers**. Click **Change/Remove**. Select **Remove** and click **Next**. Click **Yes** to confirm that you wish to uninstall Policy Patrol. After removing the Policy Patrol program you will need to restart the IIS services. Click **Yes** to restart the services. When the wizard is ready, click **Finish**.

Step 2. Install Policy Patrol

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework 1.1 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 **Yes** to accept the agreement.
4. Enter the user name and company name. Click **Next**.
5. Select the setup 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 only**. If you wish to install only certain components of the program, select **Custom**. Click **Next** to continue.
6. **If you selected Custom:** A list of features will appear. Select which features you wish to install and click **Next**.
7. Select the destination folder for the Policy Patrol installation. By default the program is installed in C:\Program Files\Red Earth Software\Policy Patrol Email 4. If you wish to change the location, click **Browse** and select another folder. When you are ready, click **Next**.
8. Specify whether Policy Patrol is installed on an Exchange 2003 machine, an Exchange 2000 machine or a separate machine (for Exchange 5.5 and Lotus Notes/Domino). Click **Next**.



9. **If you have multiple virtual SMTP servers an additional dialog will be shown:** Select the virtual SMTP server(s) that you wish Policy Patrol to monitor. Click **Next**.
10. Verify the location of your SMTP pickup directory. Policy Patrol automatically enters the path to the default pickup folder. If your pickup directory is located elsewhere, browse to the correct folder. Click **OK**.
11. Specify the notification settings. Enter the From:, To:, Cc: and Bcc: fields for the Policy Patrol notification emails. Spam reports will also be sent to these email addresses. The display name is already configured as Administrator, but you can change this as follows: "Display name" <email address>, i.e. "Joe Bloggs" <jbloggs@bloggsco.com>. Click **Next**.
12. **Only if you are installing on Exchange 2000 or 2003:** Specify a domain account (existing or new) for the Policy Patrol Folder Agents. The account will be used to run the 'Policy Patrol Agent Manager' service. If you entered a new account name, Policy Patrol will automatically create the new account and will add the account to the Local Administrators group and give it service start up rights and full rights to the Exchange information store. If you want to use an existing domain account, uncheck the box **Create a new user account**. Click **Next**.
Note: If you create a new user account and do not enter a sufficiently complex password an error message will appear asking you whether you wish to continue. When installing on Windows Server 2003, you must select **No** and re-enter a password that meets with Windows 2003 password policy.
13. Enter the external IP address and port number of the Internet Information Services (IIS) Default Web site in the following format: IP address:port number, i.e. 66.46.105.7:80. This website will be used for the challenge/response system (if you do not want to install the challenge/response website you can go back and select **Custom** as the setup type). Click **Next**.
14. A list with your installation settings will appear. Confirm that you wish to proceed with the installation by clicking **Next**.
15. Policy Patrol will now start copying the files. When Policy Patrol is ready, click **Finish** to exit the wizard.
16. If you selected to run the Policy Patrol Administration console, a screen will pop up asking you to select a license. If you are evaluating Policy Patrol, select **Policy Patrol Spam Filter 30-day evaluation** (If you later wish to try out a different Policy Patrol version you can go to <server name> > **Security** > **Licenses**, select the license and click **Remove** and **Close**. Policy Patrol will disconnect from the installation. When you connect again, Policy Patrol will allow you to select a new evaluation license type). If you have purchased Policy Patrol, enter your serial number or click on the **Paste** button to paste it from clipboard. Click **OK**.
17. The Import users wizard will pop up (not if you selected Policy Patrol Archiver). Select your import source (Active Directory, Exchange 5.5, Lotus Domino or Manual input) and click **Next**. 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. Click **Next**. If you have Exchange Server you will be able to enable users' junk mail folders in Outlook for Policy Patrol to forward spam to. Specify the junk mail folder name and click **Finish**. If you are having problems enabling junk mail folders, please consult the following KB articles: 'I am having problems enabling the junk mail folders' (<http://www.policypatrol.com/kbarticle.asp?prodid=11&id=238>) and 'How do I enable junk mail folders for Exchange 5.5?' (<http://www.policypatrol.com/kbarticle.asp?prodid=11&id=250>).

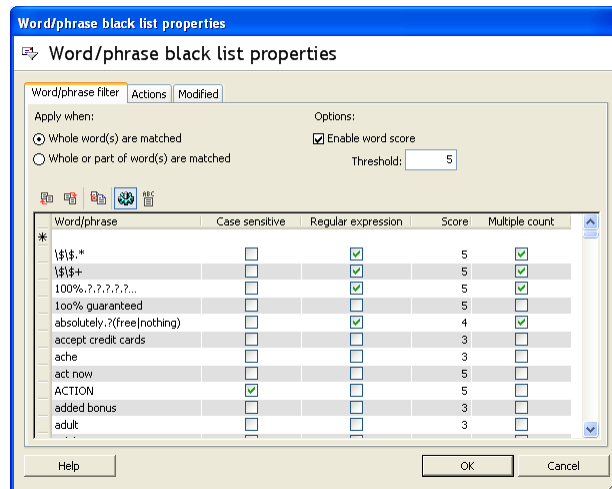
Step 3. Configure Anti-Spam

Note: Policy Patrol will start blocking spam straight after installation.

Default anti-spam configuration

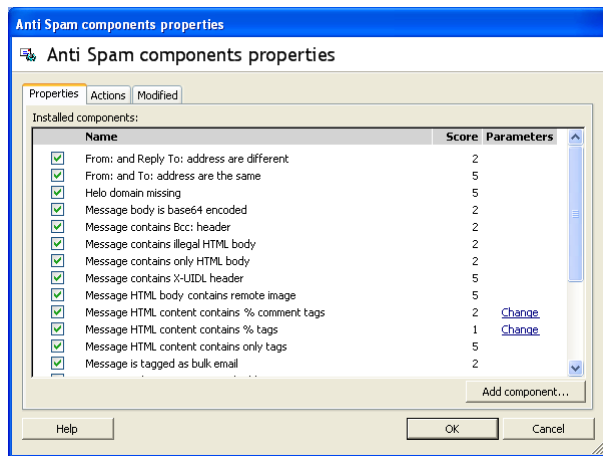
Policy Patrol Spam Filter comes with a default anti-spam configuration that can block spam right out of the box. The following options are configured:

- DNSBL lists: Policy Patrol includes several preconfigured DNSBL lists, of which some are enabled by default. If the sender is listed on an enabled list, the email is quarantined in the 'Spam (black lists)' monitoring folder.
- SURBL list: If a URL in the message is listed, the email is quarantined in the 'Spam (black lists)' monitoring folder.
- Sender Policy Framework (SPF): If the sender domain returns a Hard fail, the email is quarantined in the 'Spam (other)' monitoring folder.
- Bayesian filtering: Automatic Bayesian filter learning is enabled (i.e. all outgoing mails apart from non-deliverable reports and out-of-office replies will be added to the legitimate database) and more than 1000 spam messages have been imported into the Bayesian spam database.
- Word/phrase black list: If the message meets the word score threshold, it is quarantined in the 'Spam (other)' monitoring folder.



- Email/domain address white list: Automatic white list learning is enabled, so that recipients of each outgoing mail (apart from non-deliverable reports and out-of-office replies) are added to the white list.

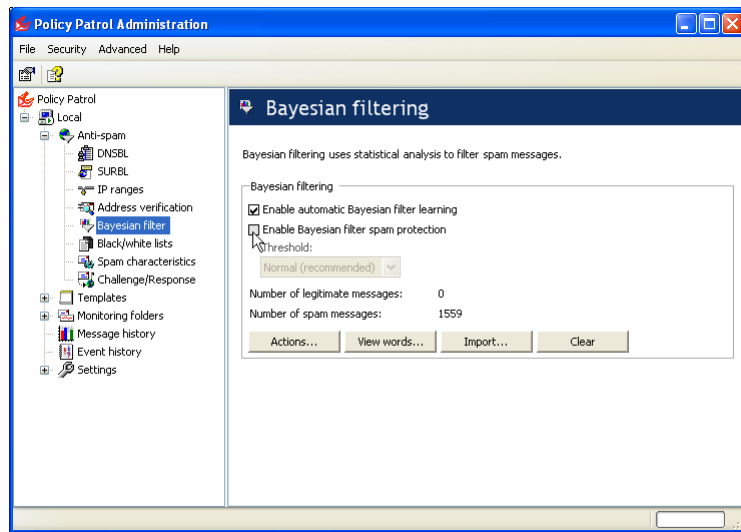
- **Spam characteristics:** If the email meets the threshold, the email is quarantined in the 'Spam (other)' monitoring folder.



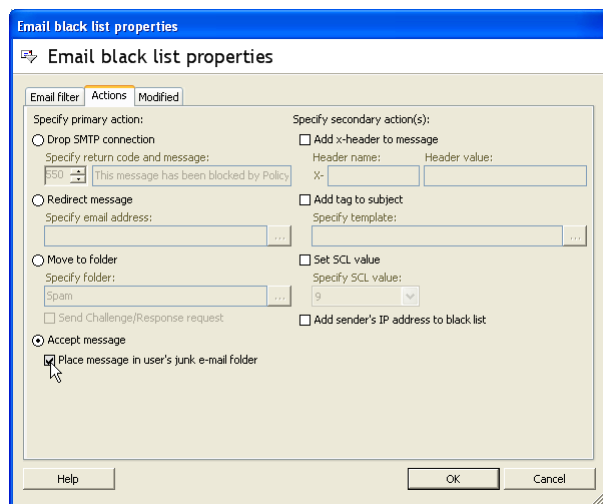
- **Challenge/Response:** If for any of the spam blocking methods you select the primary action **Move to folder** and tick the option **Send challenge/response request**, Policy Patrol will quarantine the mail and send a challenge/response email using the default template. As soon as the sender verifies their identity, the message will automatically be delivered.

What you still need to do:

- **Bayesian filtering:** Before you enable Bayesian filtering, you must 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 **Bayesian filter** and select **Enable Bayesian filter spam protection**.



- **Recipient verification:** Policy Patrol can reject messages without a valid recipient address, saving bandwidth and disk space. To do this, you must configure a lookup point that contains all your valid email addresses; Go to **Address verification**. In **Recipient verification**, click **New**. Select the Lookup method (Active Directory, Exchange 5.5 or Other LDAP service (for Lotus Domino). Click **Next**. Specify your server and domain details and click **Finish**. Repeat this for every different lookup method you wish Policy Patrol to use. You can also block directory harvest attacks by checking the option **Enable address harvesting protection**.
- **White list:** Enter email addresses and/or domains of newsletters and customers that you wish to let through by going to **Black/white lists** and clicking on the **Properties** button of the **Email/domain addresses** white list.
- **Languages:** Configure blocked languages from **Spam characteristics** > **Languages**. For instance if you wish to allow all messages apart from emails that use Chinese or Korean code pages, enable the option **Accept all messages except those using the following languages**. Then click on **Add** and select Chinese and Korean. Click **OK**.
- **Folder agents:** If you wish to make use of public folders or mailboxes in order to allow users to update white and black lists, you can do so by creating folder agents. For instructions on how to do this, please consult the manual. Note that folder agents can only be configured if you have installed Policy Patrol on Exchange 2000 or 2003.
- **Forward to junk mail folder:** If you wish Policy Patrol to forward spam mails to the users' junk mail folders, select the primary action **Accept message** and tick the option **Place message in user's junk e-mail folder** for each spam filtering method. Note: This option requires Exchange Server 5.5, 2000 or 2003. In addition, for this to function correctly you should have enabled junk e-mail folders while importing users into Policy Patrol. If you did not, you can enable junk mail folders by going to **Settings** > **Users**, selecting the user, right-clicking and selecting **Enable junk e-mail folder**.

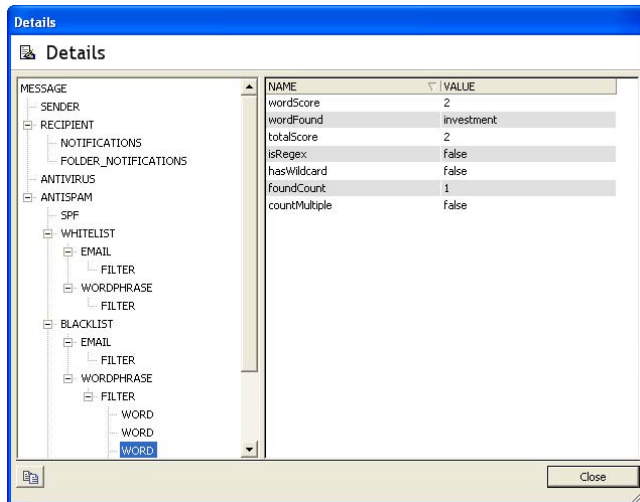


Policy Patrol includes more anti-spam features, such as IP address blocking and Email/domain address black lists. For more information on how to configure these options, please consult the product manual.

In order to help you fine tune your spam filtering, Policy Patrol includes detailed information on each message that was processed and quarantined.

Quarantined messages

If you want more information on why a message was quarantined, go to the respective Monitoring folder. Select the message, right-click and choose **Details....** A dialog will appear including detailed information on the results of each spam filtering method and if relevant any words found and their score.



All messages

If you want more information on a particular message that was processed by Policy Patrol, go to **Message history**. Message history displays a list of the last 1000 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 report in the bottom pane. To get more detailed information, right-click and choose **Details**. This can be useful if for instance you want to find out why a message was not quarantined.

Step 4. 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.

4906 El Camino Real, Ste 209
Los Altos, CA 94022-1444
United States
Toll-free: 1-800-921-8215
Phone: (650) 967 1011
Fax: (650) 887 0470
Sales: sales@reearthsoftware.com
Support: support@reearthsoftware.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@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- 2006 by Red Earth Software.