Quick Start

Policy Patrol Mail Security 10

This guide will help you start using Policy Patrol Mail Security 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
- ☑ Microsoft Exchange Server 2003, Windows Small Business Server 2003, or Lotus Domino R5-R8 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 (64-bit version):

- ☑ Windows Server 2003, 2008/2008 R2, 2012/2012 R2.
- ☑ Microsoft Exchange Server 2013, 2010, 2007 or Windows Small Business Server 2008/2011.
- ☑ 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 64-bit can be installed on an **Exchange 2007/2010/2013** machine with one of the following roles:

- Hub Transport Role
- Edge Transport Role (with access to Active Directory)

Note: For Outlook Sent Items to be updated, Policy Patrol must be installed on an Exchange Server machine with the Hub Transport Role (not an Edge Transport Role).

⇒ If you are not installing Policy Patrol on the same machine as Exchange Server, Policy Patrol will not process internal mails or be able to update Outlook Sent Items with email signatures and other modifications. In order to install Policy Patrol on a

non-Exchange Server machine you must follow the instructions for installing Policy Patrol on a **separate machine**:

 Installing Policy Patrol on a separate machine
(http://www.policypatrol.com/assets/pp10-separatemachine.pdf)

⇒ If you have **Lotus Domino R5-8 Mail Server** (or another mail server), you must install Policy Patrol on a separate machine. Policy Patrol does not offer internal mail filtering for Lotus Domino or updating of Outlook Sent Items. 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/assets/pp10-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). If you are installing Policy Patrol 64-bit in a cluster, there are no specific cluster instructions to follow; You can perform a regular installation as described in step 2:

 Installing Policy Patrol in a cluster
(http://www.policypatrol.com/assets/pp10-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.

⇒ 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.

⇒ If you have **Policy Patrol 7 or 8** installed, you can perform an upgrade to version 9 whilst keeping your existing configuration. For further instructions on this, please consult the following document:

 Policy Patrol 10 Upgrade Guide
(http://www.policypatrol.com/assets/pp10-upgradeguide.pdf)

⇒ If you have **Policy Patrol 4, 5 or 6** installed, you can keep your configuration but you must first upgrade to version 7 before you upgrade to version 10. For further instructions on how to upgrade to Policy Patrol 7, please consult the following document:

Policy Patrol 7 Upgrade Guide
(http://www.policypatrol.com/assets/pp7-upgradeguide.pdf)

⇒ If you have **Policy Patrol 1, 2 or 3** installed, it is not possible to use your existing configuration files in version 10.

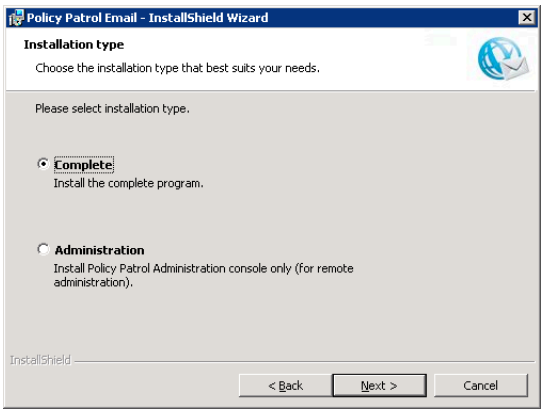
Step 2. Install Policy Patrol

1. Double-click on **PolicyPatrol.exe** (32-bit version) or **PolicyPatrol64.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 install 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 console**.



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**.

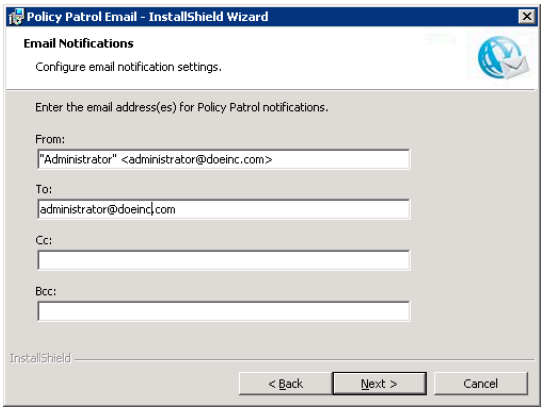
6. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Mail Security** and click **Next**.

   Note: If you are evaluating Policy Patrol and wish to try out a different Policy Patrol edition after the installation, you can go to **Policy Patrol Administration** > **<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.

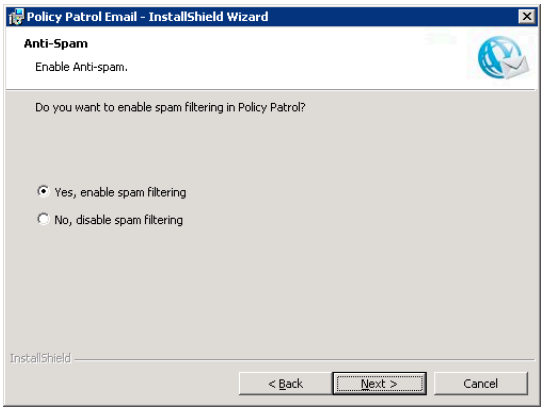
7. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email (32-bit version) or C:\Program Files (x86)\Red Earth Software\Policy Patrol

Email (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 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**.



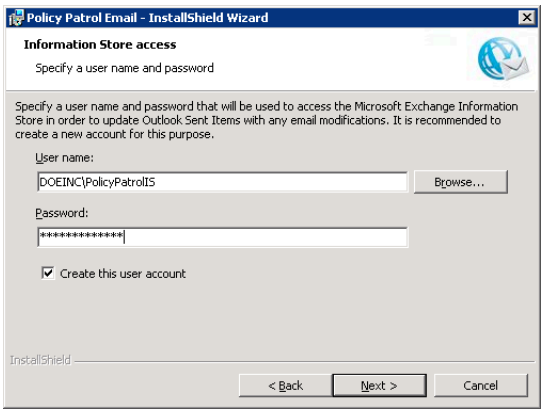
9. Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected **No, disable spam filtering**, continue to step 12.



10. **If you selected to enable spam filtering**: 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**.

11. 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**.

12. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please note that if you want to use an existing account instead of creating a new one, that this account cannot be a member of the Administrators group in Active Directory. If the account does not yet exist, leave the option **Create this user account** enabled so that Policy Patrol will automatically create the user account. When you are ready, click **Next**. Note that this dialog only appears if you are installing Policy Patrol on an Exchange Server 2003, 2007, 2010 or 2013 machine.



13. Click **Install** to start installing.

14. When the installation wizard has finished copying the files, click **Finish**.

15. The configuration wizard will now start up. Click **Next** in the Welcome screen.

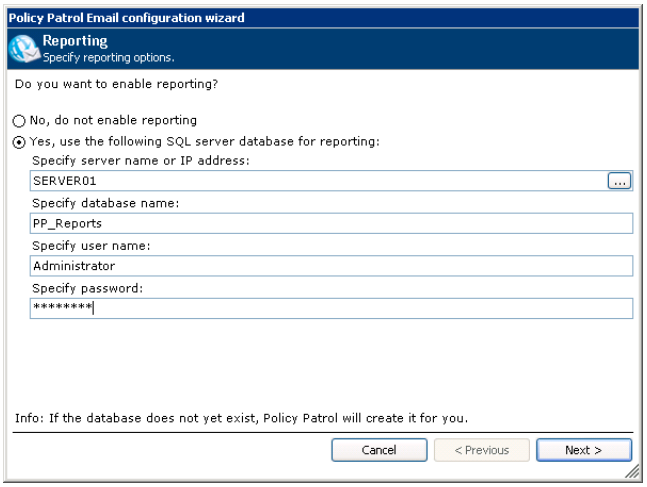
16. Specify the location from where you would like to import your users (Active Directory, Lotus Domino or Manual input) and click **Next**. (Note: the 64-bit version only includes the Active Directory and Manual Input options.)

17. 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 detailed information on the different options in this dialog, please consult the product manual. Click **Next**.

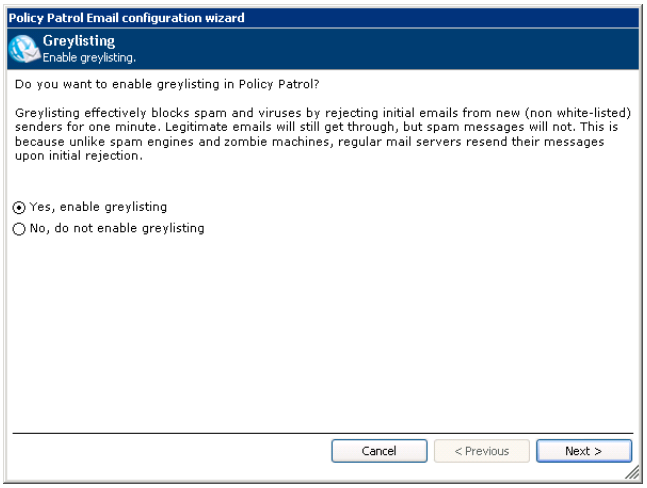
18. Select whether you wish to enable Mail Backup. If you enable Mail Backup you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically 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.

19. 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.

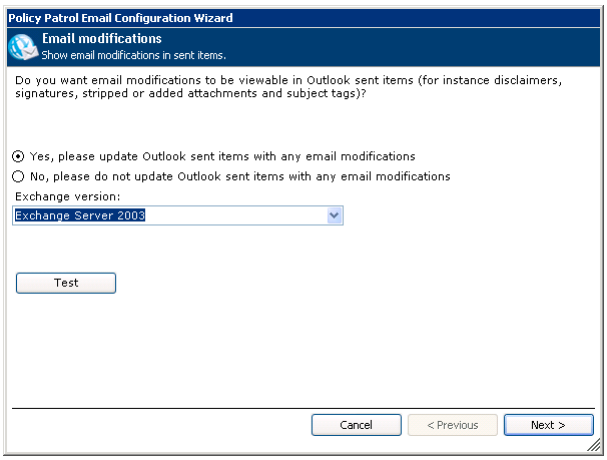


20. Select whether you wish to enable greylisting. Greylisting effectively blocks spam and viruses by initially rejecting messages from new, non white-listed senders for one minute, therefore allowing legitimate emails through without any user intervention, and blocking the non-legitimate emails. Select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

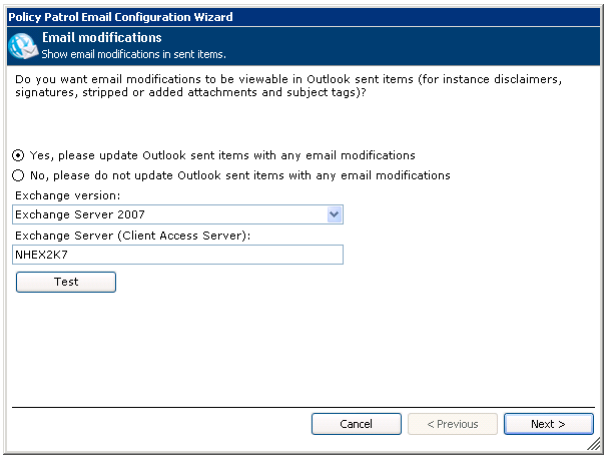


21. Select whether you wish to view email modifications in Outlook Sent items. If you select **Yes**, any modifications that are applied to outgoing emails by Policy Patrol, such as disclaimers, signatures, subject tags and adding or stripping attachments, will automatically show in Outlook Sent Items (after a few seconds the message in Sent Items will be replaced with the actual message that was sent). Depending on your Exchange Server version, a number of options will be shown.

    If you have Exchange 2003: In 'Exchange version', Exchange Server 2003 should be selected.



If you have Exchange 2007/2010/2013: In 'Exchange version', your Exchange version should be selected (Exchange Server 2007, 2010 or 2013). In 'Exchange Server (Client Access Server)' the name of your Exchange Client Access Server should be listed. If you only have one Exchange Server, the name of the local server should be listed. If you have multiple Exchange Servers, you need to enter the name of your Client Access Server.



When you are ready, click **Next**. Note: This dialog does not appear if Policy Patrol is not being installed on Exchange Server 2013, 2010, 2007, or 2003.

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

Step 3. Configure Anti-Spam & Anti-Phishing

If you selected to enable anti-spam, Policy Patrol will start blocking spam & phishing emails 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

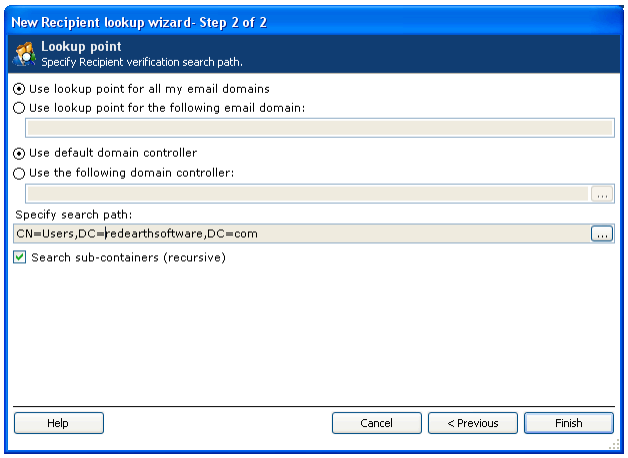
Policy Patrol Spam Filter is preconfigured to stop spam right out of the box using a number of spam blocking techniques including DNSBL lists, SURBL lists, Sender Policy

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:

1. 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.
2. 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.

3. 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.



4. 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**.
5. 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**.

Policy Patrol includes more anti-spam features, such as country blocking, IP address blocking, challenge/response, 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.

Spam management

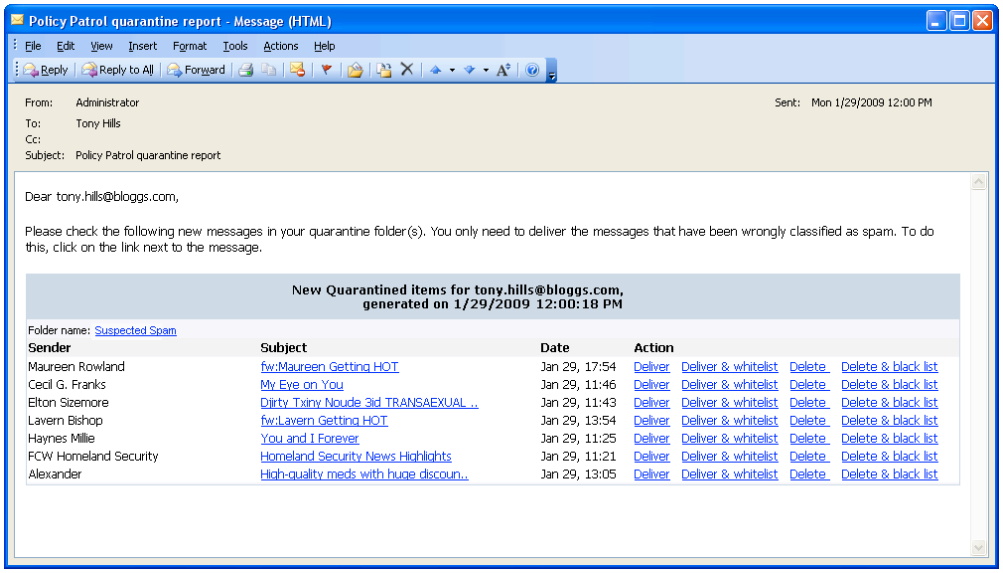
If you want your users to be able to manage their own spam you can configure a quarantine report to be sent to the users including newly quarantined items, and you can provide them with access to the Policy Patrol Web Manager:

- 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 (Administrators will be able to see all users' emails). The Policy Patrol Web Manager can be accessed from the following link: http://<servername>/PolicyPatrolEmail (where <servername> is the name of the Policy Patrol machine). In **Settings** > **Web manager options** you can select whether you wish to allow users to add email addresses and/or domains to white lists and black lists and/or to add entries only to their individual white lists and black lists. A Policy Patrol Web Manager user guide and a sample user memo that you can use to

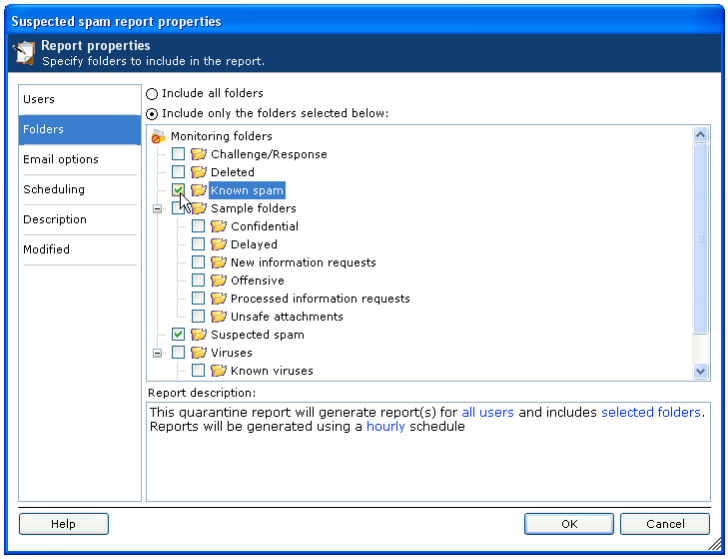
inform your users about the new spam management system are available for download from the following links:

Sample user memo
(http://www.policypatrol.com/assets/pp10-usermemo.doc)

Policy Patrol Web Manager User guide
(http://www.policypatrol.com/assets/pp10-userguide.doc)



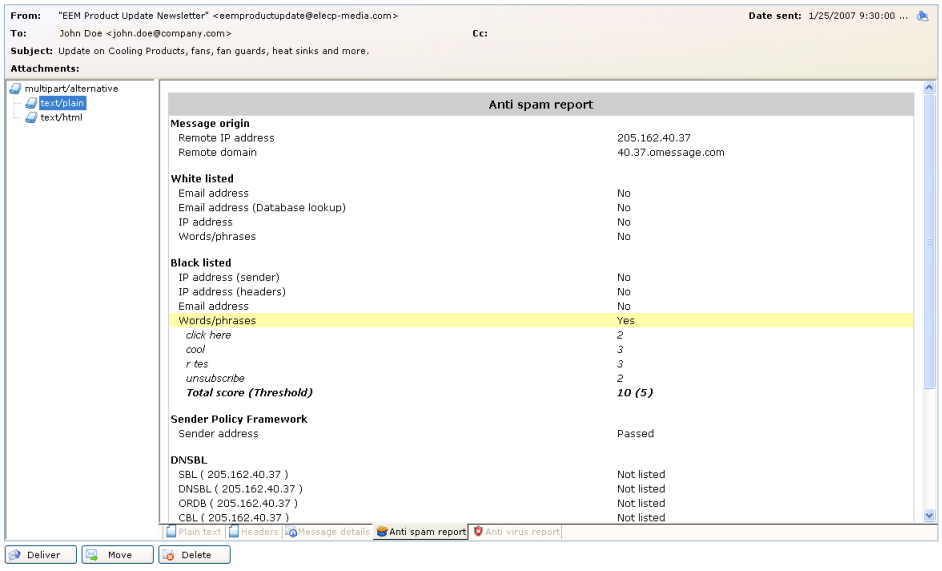
- Quarantine report (requires Web Manager): Policy Patrol includes a sample quarantine report that sends a list of newly quarantined items in the Suspected spam folder once a day. To enable this report for all users, go to **Monitoring folders** > **Quarantine reports**. Right-click on the **Suspected 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.

Message 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.

Step 4. Enable Metascan Multi Anti-Malware Scanning

With the Metascan add-on, Policy Patrol Mail Security can scan email attachments with multiple (between 4 and 40) antimalware engines at once, significantly increasing the virus detection rate while maintaining fast scanning performance. Metascan can also perform file sanitization and file type checking, preventing zero-day and targeted attacks. Metascan is available as a server application that you install within your network (Metascan On-Premise), or as a cloud-based deployment that scans files in the cloud (Metascan Online). Download a trial version of Metascan On-Premise (http://www.policypatrol.com/policy-patrol-mail-security/download-metascan) or request your free Metascan Online subscription (http://www.policypatrol.com/request-free-metascan-online).

Step 5. Configure Disclaimers and Signatures

To configure a disclaimer or signature, go to **Rules** > **Disclaimer rules**. Select the appropriate folder and click **New**. The Rules wizard will guide you through the users, directions, conditions, exceptions and actions for the rule. To add a disclaimer, in Rule Actions, click on **Modify message** and select the action **Add disclaimer/signature**.

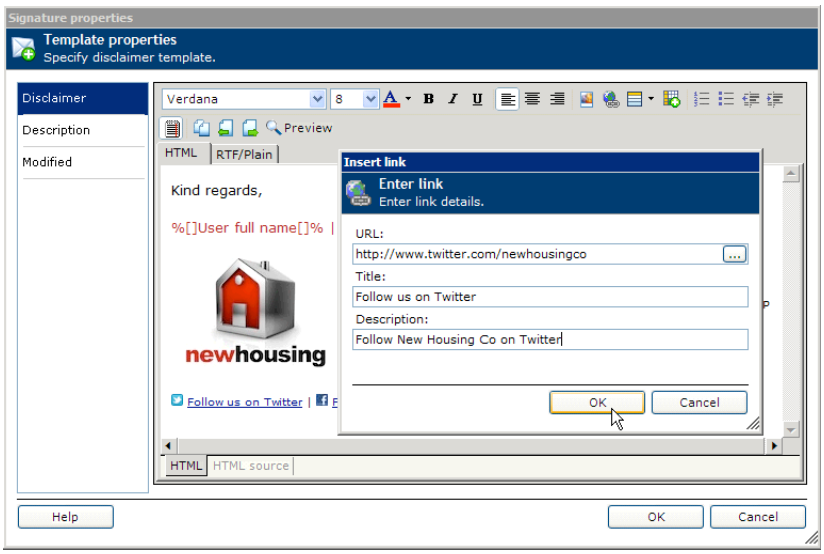
A dialog will pop up where you can select the type of disclaimer/signature you wish to add:

Add disclaimer/signature: Your email disclaimer/signature template is added to the top or bottom of your email message.

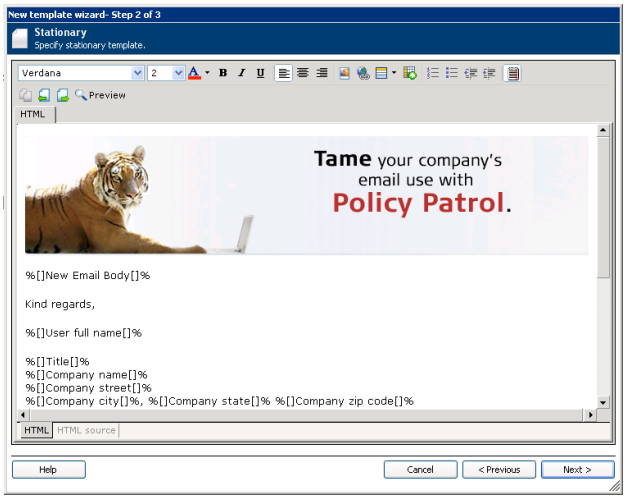
Add disclaimer/signature and format entire email (HTML only): Your email message is inserted into your HTML Stationary template.

In this dialog there are further options including avoiding multiple disclaimers, placing the disclaimer/signature after the most recent message text and using a subject code to add/suppress a disclaimer/signature.

The program already includes a number of sample disclaimers and signatures in **Settings** > **Templates** > **Sample templates**. You can edit these or create your own. The disclaimer templates can include formatting, pictures and Active Directory merge fields that are replaced with the user's Active Directory Properties. You can even use QR Codes and insert the sender's Avatar into the email signature.



Example of a standard disclaimer/signature template



Example of an HTML Stationary template

Note that the only difference between the standard Disclaimer template and the HTML Stationary template is that the latter includes the following merge fields:

%[]New Email Body[]%: This field will be replaced with the most recently entered message text, i.e. the email text above the first message separator.

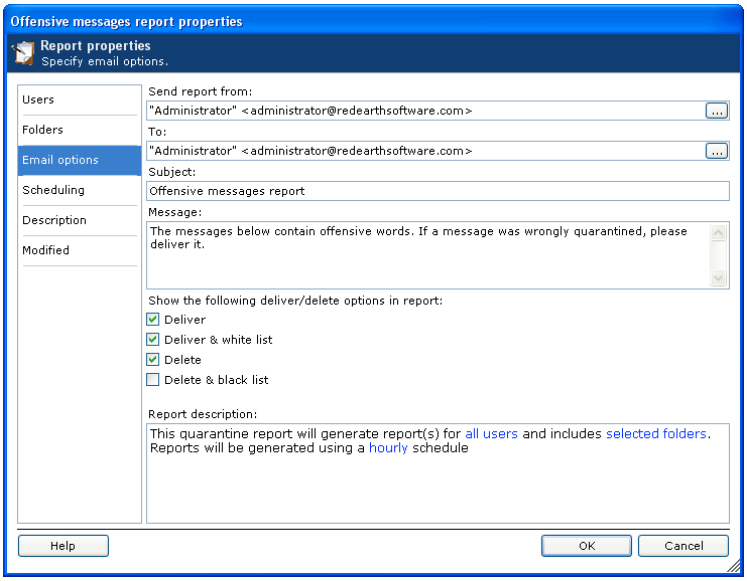
%[]Previous Email Body[]%:This field will be replaced with the previous message text, i.e. the email text below the first message separator.

It is also possible to add a random disclaimer/signature by selecting the secondary action **Add random disclaimer/signature**. Policy Patrol will then rotate your disclaimers and signatures by randomly adding any disclaimer or signature template that exists in the selected folder.

Step 6. Configure Email Content Policies

To create a new content policy, go to the **Email Content Policies** node, select the appropriate folder and click **New**. The Policy wizard will guide you through the users, directions, conditions, exceptions and actions for the rule. The program already includes a number of sample rules. You can edit these or create your own.

Tip: If you are quarantining messages that meet certain conditions, for instance messages that contain offensive or confidential content, it is a good idea to configure a quarantine report that sends a message to the manager or Administrator with the emails that were quarantined. This allows the reviewer to check the quarantined emails and take appropriate action. Note that for a user to be able to view another user's emails, you must create an Administrator quarantine report. A sample 'Offensive messages report' is already configured in **Quarantine** > **Quarantine reports**. To enable it, right-click and choose **Enable**. Note that the quarantine report requires the Policy Patrol Web Manager to be installed. If you do not have this installed you can install it by going to **Start** > **Settings** > **Control Panel** > **Programs and Features** and modifying the Policy Patrol installation.



Step 7. More information

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

1. No disclaimers/signatures are being added
2. User merge field is not being replaced
3. Avoid multiple disclaimers is not working
4. I'm having problems enabling the junk mail folder
5. Spam filter is letting spam through
6. White listed messages are still being blocked
7. Outlook Sent Items are not being updated
8. Does Policy Patrol support clustering?
9. If I purchase do I need to reinstall the software?

10. Policy Patrol is not processing any messages

The answers to these questions and more can be found in our knowledge base at: https://support.redearthsoftware.com/forums.

⇒ For more information on how to configure Policy Patrol, please download the product manual from: http://www.policypatrol.com/documentation.

⇒ If you have any technical or configuration questions please send an email to: support@redearthsoftware.com.

⇒ If you require any assistance, please contact us at one of the following offices:

Red Earth Software, Inc.
4845 Pearl East Circle, Ste 101
Boulder, CO 80301
United States
Toll-free: 1-800-921-8215
Phone: (408) 370 9527
Fax: (408) 608 1958
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)20-8328 9830
Fax: +44-(0)20-8711 5771
Sales: sales@redearthsoftware.co.uk
Support: support@redearthsoftware.co.uk

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2014 by Red Earth Software.