



MANUAL

# Policy Patrol

---

This manual, and the software described in this manual, are copyrighted. No part of this manual or the described software may be copied, reproduced, translated or reduced to any electronic medium or machine-readable form without the prior written consent of Red Earth Software except that you may make one copy of the program solely for back-up purposes.

Policy Patrol® is a registered trademark of Red Earth Software™. All product names referenced in this documentation belong to the respective companies.

Copyright © 2001-2003 by Red Earth Software. All rights reserved.

# Table of Contents

## **Introduction ..... 4**

*Why do you need Policy Patrol?.....4*

*Policy Patrol features .....4*

*System requirements.....6*

## **Installing Policy Patrol ..... 7**

*If you have Exchange 2000 .....7*

*If you have Exchange 5.5.....7*

*If you have Lotus Domino or another mail server .....8*

*If you have a clustered environment.....8*

    Create the Mail Processor cluster resource: .....9

    Only if you want to use scheduled synchronization:  
    .....10

    Only if you want to use remote administration: .....10

    Only if you want Policy Patrol to check for new  
    updates: .....11

*If you have a frontend/backend server setup ..... 12*

*If you have Policy Patrol 1.x installed..... 12*

*Installing Policy Patrol on a separate machine..... 12*

*Installation ..... 15*

*Policy Patrol Configuration wizard ..... 17*

*Remote administration ..... 22*

*Creating Connectors ..... 23*

*Licensing ..... 26*

    Policy Patrol Disclaimers ..... 26

    Policy Patrol Enterprise ..... 26

*Add license ..... 26*

*Licensed users ..... 27*

*Policy Patrol Update Wizard ..... 27*

*Services ..... 28*

## **Configuring rules.....30**

*Configuring a new rule .....30*

    Step 1. Which users should this rule apply to? .....30

    Step 2. Which messages do you want to check? ....31

    Step 3. Which conditions should be met? .....32

    Step 4. Should this rule have exceptions? .....42

    Step 5. What actions should be taken?.....43

        Primary actions .....43

        Secondary actions .....44

        Ordering of secondary actions.....51

    Step 6. Should this rule be scheduled?.....51

    Step 7. Enter a name for the rule.....52

*Editing existing rules.....53*

*Ordering rules .....53*

    Processing speed.....53

    Ordering result.....54

    Continue processing .....54

*Ordering conditions.....55*

*Ordering secondary actions.....55*

## **Creating Filters .....56**

*Creating a Word/Phrase filter .....56*

*Creating an Attachment Name filter .....58*

*Creating an Attachment Type filter.....59*

*Creating a Domain/Email Address filter .....59*

*Editing filters.....60*

<b>Creating Templates.....</b>	<b>62</b>
<i>Creating a Notification template .....</i>	62
<i>Creating a Tag template .....</i>	64
<i>Creating a Disclaimer template.....</i>	65
<i>Editing templates .....</i>	67
<i>Fields.....</i>	67
User fields.....	67
Message fields .....	68
DSN fields .....	69
Rule fields .....	70
Date/Time fields .....	70
<b>Monitoring messages.....</b>	<b>72</b>
<i>Monitoring messages from Policy Patrol.....</i>	72
Last 50 messages processed by Policy Patrol .....	72
Viewing quarantined, delayed and deleted messages .....	72
Saving down and deleting attachments .....	74
Removing body parts.....	74
Adding senders and recipients to filters.....	75
Accepting messages on hold .....	75
Rejecting messages on hold .....	76
Undeleting deleted messages .....	76
<i>Monitoring messages via the web .....</i>	76
<i>Monitoring messages via email.....</i>	76
<b>Archiving .....</b>	<b>78</b>
<i>SQL archiving .....</i>	78
<i>Creating an archive .....</i>	78
<i>How to archive messages .....</i>	80
<i>Viewing archived attachments.....</i>	81
<b>Reporting &amp; logging.....</b>	<b>82</b>
<i>Logging.....</i>	82
<i>Creating a report template .....</i>	82
<i>Generating a report .....</i>	87
<b>Spam blocker.....</b>	<b>88</b>
<i>Spam lists .....</i>	88
<i>Configuring the spam blocker.....</i>	88

<i>Creating rules for spam messages .....</i>	90
<b>Virus checking.....</b>	<b>91</b>
<i>Kaspersky™ Anti-Virus .....</i>	91
<i>Installing Kaspersky™ Anti-Virus .....</i>	91
<i>Configuring Anti virus.....</i>	93
<i>Configuring rules for virus checking .....</i>	94
<b>Advanced options.....</b>	<b>95</b>
<i>General .....</i>	95
<i>Local domains .....</i>	95
Add and remove local domains.....	95
Auto detect local domains .....	95
Exclude IP addresses .....	96
<i>System directories .....</i>	96
<i>Message flow logging .....</i>	96
<i>System logging .....</i>	96
<i>System notifications.....</i>	97
<i>User fields .....</i>	97
<i>Code pages.....</i>	99
<i>Attachment checking.....</i>	99
<i>Attachment spoofing .....</i>	99
<i>Delivery notifications.....</i>	99
<i>Advanced .....</i>	100
<b>Sample rules .....</b>	<b>101</b>
<i>Delete messages from the Spam senders filter .....</i>	101
<i>Delete all mails from re-offending virus senders .....</i>	102
<i>Delay large messages .....</i>	102
<i>Add re-offending virus senders to filter.....</i>	102
<i>Quarantine viruses that cannot be deleted .....</i>	102
<i>Quarantine suspected viruses.....</i>	103
<i>Quarantine all scripts .....</i>	103
<i>Quarantine offensive content.....</i>	104
<i>Block dangerous attachment types.....</i>	104
<i>Block spoofed attachments .....</i>	104
<i>Notify when virus is cleaned or deleted.....</i>	105
<i>Add signature.....</i>	105
<i>Add external disclaimer .....</i>	105
<i>Add internal disclaimer .....</i>	106
<i>Automatically create white list.....</i>	106
<i>Add tag to spam messages .....</i>	106

<i>Customize Delivery Status Notifications</i> .....	108
<i>Remove [No disclaimer] from the subject</i> .....	108
<i>Compress attachments larger than 1 MB</i> .....	108
<i>Archive all mails</i> .....	108
<b>Troubleshooting</b> .....	<b>110</b>
<i>System Events</i> .....	110
<i>Knowledge Base</i> .....	110
Will Policy Patrol search embedded emails? .....	110
User field is not working .....	110
My disclaimer attachment is empty .....	111
My rule that searches for words/phrases always triggers.....	111
Why is the message size not the same as in Outlook or Quarantined items? .....	111
How do I enable remote administration after installation?.....	111
Inline pictures are treated as attachments .....	112
Can I undelete deleted messages? .....	112
Can Policy Patrol retrieve Exchange 5.5 distribution lists? .....	112
Will Policy Patrol automatically retrieve and license new users?.....	112
I can no longer see the tree nodes Monitoring, Reporting, Archiving, Anti-virus and Spam blocker .....	112
Are attachment names case sensitive?.....	112
I have not made any changes but still Policy Patrol asks to commit changes.....	112
I cannot enable my rule .....	112
Can Policy Patrol also check email addresses in the bcc: field? .....	113
<i>Support Wizard</i> .....	113

## Introduction

**P**olicy Patrol is a comprehensive email-monitoring tool that can check internal as well as external emails and block viruses, spam, hoaxes, confidentiality leaks, scripts, offensive content, add disclaimers and much more.

### Why do you need Policy Patrol?

Companies are increasingly using email as their main communications tool. Email offers a substantial number of advantages above conventional means of communication: it is fast, efficient, cost effective, universal and international. However by giving employees access to email, companies are also running certain risks, such as:

- Confidentiality breaches
- Legal liability
- Damage to reputation
- Lost productivity
- Network congestion
- Email retrieval on court order

In combination with a sound email policy, Policy Patrol helps companies protect themselves against these threats and gain more control over their email system.

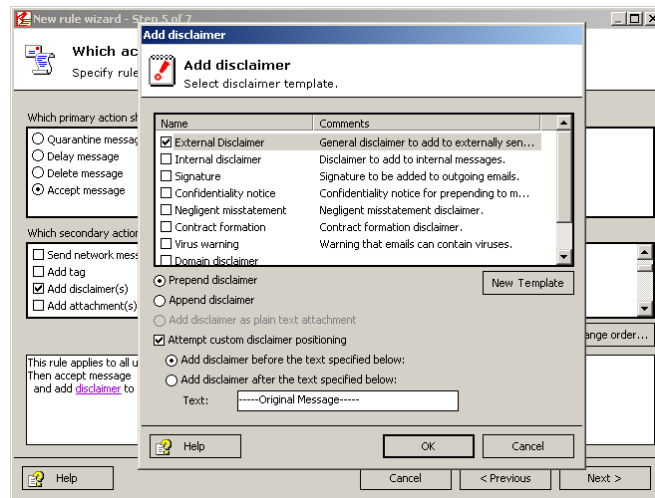
### Policy Patrol features

Policy Patrol offers the following features:

- Intelligent keyword filtering using word scores.

## INTRODUCTION

- ☑ Attachment checking based on words/phrases, size, name, type, number of attachments and spoofing.
- ☑ Spam blocking (real-time blacklists and spam header & keyword filtering).
- ☑ Virus scanning with Kaspersky™ Anti-virus engine.
- ☑ Disclaimers & signatures (append, prepend or custom positioning, and optionally with merge fields, formatting, pictures & attachments).



- ☑ Delaying of messages.
- ☑ Send blind copy.
- ☑ Filtering on domains and email addresses.
- ☑ Approval or rejection of quarantined messages via email, the web or remote installation.
- ☑ Reports on email usage and rule statistics
- ☑ Archiving (including attachments).
- ☑ Billing codes to apportion email costs.
- ☑ Auto printing of emails.
- ☑ Compression and decompression.
- ☑ Customization of NDRs (Non-deliverable reports) and Delivery Status Notifications (DSN).
- ☑ Converting HTML/rich text messages into plain text.

## INTRODUCTION

- ☑ Email and network notifications.
- ☑ Email management features, such as adding a business card (vCard) or attachment, sending auto replies, removing words from a subject, adding recipients or senders to a filter, adding an X-header, changing message priority, removing read/delivery receipt requests and running a program.

## System requirements

Policy Patrol requires the following to be installed:

- ☑ Windows 2000 Professional, Server or Advanced server or Windows XP Professional.
- ☑ Exchange Server 2000/5.5, Lotus Notes/Domino or other mail server.
- ☑ Microsoft .NET Framework (If you do not have this installed the Policy Patrol program will download and install it for you).



## Installing Policy Patrol

**T**his chapter describes the steps for installing Policy Patrol on the mail server machine and a separate machine. It also discusses how to enter your serial number and use the update wizard.

### If you have Exchange 2000

If you have Exchange server 2000, it is recommended to install Policy Patrol on the Exchange server machine (proceed to 'Installation' paragraph). It is also possible to install Policy Patrol on a separate Windows 2000 machine, but in this case Policy Patrol will not be able to process your internal mails. All other features will be available. For instructions on how to install on a separate machine, see 'Installing Policy Patrol on a separate machine'.

### If you have Exchange 5.5

If you have Exchange 5.5, you must install Policy Patrol on a separate Windows 2000 machine. Policy Patrol will offer the same functionality for Exchange 5.5 as for Exchange 2000, with the exception that internal mail will not be processed. Policy Patrol can retrieve your users & groups (including user properties for merge fields) from Active Directory or Exchange 5.5. If you retrieve your users from Exchange 5.5, make sure that **LDAP** is enabled in Microsoft Exchange Administrator > Organization > Site > Configuration > Protocols > Properties > LDAP. Tick **Windows NT Challenge/Response** in the Authentication Tab and in the Search tab set the **Maximum number of search results returned** to at least 10.000.

#### Info

You cannot install Policy Patrol on the same machine as Exchange 5.5, even if it is installed on a Windows 2000 machine. This is because you need to remove the Windows 2000 SMTP service to be able to start the

Exchange 5.5 Internet Mail Connector, and Policy Patrol requires the SMTP service to function.

## If you have Lotus Domino or another mail server

If you are using Lotus Notes/Domino or another mail server, you must install Policy Patrol on a separate Windows 2000 machine. Policy Patrol will offer all functionality, apart from processing internal mails. Policy Patrol can retrieve Lotus Domino users & groups, and their user properties for the user fields.

## If you have a clustered environment

Policy Patrol can be installed with Active/Passive clusters. Policy Patrol does not support Active/Active clusters. To install Policy Patrol in a clustered environment follow the next steps:

1. Ensure that the first cluster node is active and install Policy Patrol on the first node as per the instructions in the 'Installation' paragraph. After installation, run the **Policy Patrol Clustering Wizard** by going to C:\Program Files\Red Earth Software\Policy Patrol and double clicking on **PP2\_ClusterWizard.exe**.

Click **Next** in the Welcome screen. Select **First node in the cluster** and click **Next**. Enter the name and IP address of the cluster. When you are ready, click **Next**. In **Shared folder**, enter or select the shared folder to be accessed by both cluster nodes (make sure that the folder is located on a drive that is shared by the cluster). If you enter a new folder name, the wizard will automatically create it. Click **Next**. The wizard will now create a share and move the Policy Patrol configuration files to this directory. When the configuration is complete, click **Finish**.

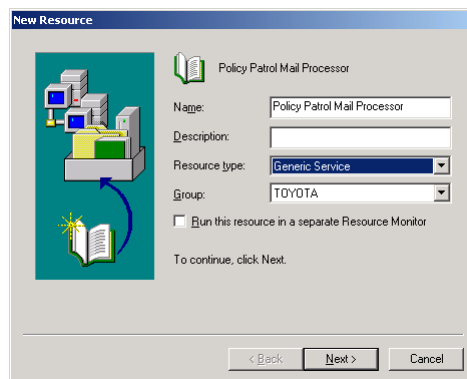
2. Now you must make the second cluster node active by going to Start > Programs > Administrative Tools > **Cluster Administrator**. Go to

**Groups.** Right-click the Exchange cluster group and select **Move Group**. The cluster will now failover and make the second node active.

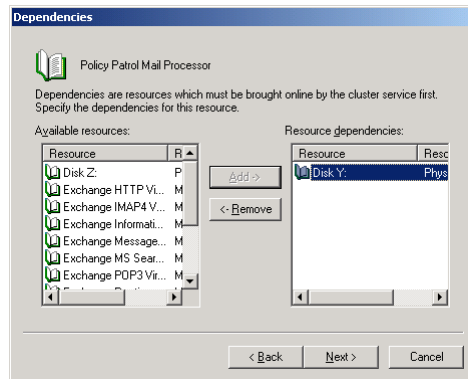
3. When all resources are online again, install Policy Patrol on the second node as per the instructions in the 'Installation' paragraph. After installing Policy Patrol, run the **Policy Patrol Clustering Wizard** by going to C:\Program Files\Red Earth Software\Policy Patrol and double clicking on **PP2\_ClusterWizard.exe**. Click **Next** in the Welcome screen. Select **Second node in the cluster** and click **Next**. Enter the name and IP address of the cluster. When you are ready, click **Next**. In **Shared folder**, select the shared folder that you configured when running the Policy Patrol Clustering Wizard on the first node. Click **Next**. The wizard will now point the Policy Patrol configuration to this directory. When the configuration is complete, click **Finish**.
4. Now create the Policy Patrol cluster resources on either of the nodes as follows:

**Create the Mail Processor cluster resource:**

- Go to Start > Programs > Administrative Tools > **Cluster Administrator**. Go to **Groups**. Right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
- Enter 'Policy Patrol Mail Processor' as the name. Select **Generic Service** as the resource type. Click **Next**.



- In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
- In 'Available resources', select the disk where the Policy Patrol shared folder is located. Click **Add** and **Next**.



- Enter `PP2_MailProcessor` as the service name and do not enter any start parameters. Click **Next**.
- Do not add any registry keys and click **Finish** to create the Policy Patrol Mail Processor cluster resource.
- Right-click the Policy Patrol Mail Processor resource in the list and choose **Bring Online**.

**Only if you want to use scheduled synchronization:**

- In the Cluster Administrator, right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
- Enter 'Policy Patrol Synchronization Manager' as the name. Select **Generic Service** as the resource type. Click **Next**.
- In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
- In 'Available resources', select the disk where the Policy Patrol shared folder is located. Click **Add** and **Next**.
- Enter `PP2_SyncManager` as the service name and do not enter any start parameters. Click **Next**.
- Do not add any registry keys and click **Finish** to create the Policy Patrol Synchronization Manager cluster resource.
- Right-click the Policy Patrol Synchronization Manager resource in the list and choose **Bring Online**.

**Only if you want to use remote administration:**

- In the Cluster Administrator, right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.

- Enter 'Policy Patrol Remote Manager' as the name. Select **Generic Service** as the resource type. Click **Next**.
- In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
- In 'Available resources', select the disk where the Policy Patrol shared folder is located. Click **Add** and **Next**.
- Enter `PP2_RemoteManager` as the service name and do not enter any start parameters. Click **Next**.
- Do not add any registry keys and click **Finish** to create the Policy Patrol Remote Manager cluster resource.
- Right-click the Policy Patrol Remote Manager resource in the list and choose **Bring Online**.

**Only if you want Policy Patrol to check for new updates:**

- In the Cluster Administrator, right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
- Enter 'Policy Patrol Update Manager' as the name. Select **Generic Service** as the resource type. Click **Next**.
- In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
- In 'Available resources', select the disk where the Policy Patrol shared folder is located. Click **Add** and **Next**.
- Enter `PP2_UpdateManager` as the service name and do not enter any start parameters. Click **Next**.
- Do not add any registry keys and click **Finish** to create the Policy Patrol Update Manager cluster resource.
- Right-click the Policy Patrol Update Manager resource in the list and choose **Bring Online**.

5. Open the Policy Patrol Administration on the active node by going to Start > Programs > Policy Patrol > Administration. Click on **Add installation**. Select **Other installation** and enter the name or IP address of the cluster. In **Port**, enter the port number that you specified during installation of Policy Patrol on the **first node** (by default 8000). Click **OK**. To start configuring Policy Patrol, select the installation you just added and click **Connect**.

## If you have a frontend/backend server setup

If you have frontend and backend Exchange 2000 servers you need to determine on which machine(s) you must install Policy Patrol according to the following guidelines:

- If you use POP3 clients on the frontend server you must install Policy Patrol on the frontend server.
- 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 Policy Patrol.

As regards licensing, you will need to purchase a license for each backend server, but not for the frontend server. To request an additional serial number for your frontend server please send an email with your purchased serial number to [orders@redearthsoftware.com](mailto:orders@redearthsoftware.com).

## If you have Policy Patrol 1.x installed

Before you install version 2, you must uninstall Policy Patrol 1.x. 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**.

## Installing Policy Patrol on a separate machine

If you don't have Exchange 2000 you must install Policy Patrol on a different machine than the mail server. If you have Exchange 2000, this is optional (remember that in this case internal mails will not be processed). Before you install Policy Patrol on a non-mail server machine you must make sure that the following is installed:

1. Windows 2000 Professional, Server or Advanced Server or Windows XP.
2. SMTP service (part of Internet Information Services): This is installed by default on Windows 2000 Server and Advanced Server and is an option on Windows 2000 Professional. To install the SMTP service, go to Start > Settings > Control Panel > Add/Remove Programs > Add/Remove Windows Components. Select **Internet Information**

**Services** and click on **Details**. Check **SMTP service**. Any other required components are checked automatically. Click **OK**. Click **Next** to install the SMTP service.

3. Microsoft .NET Framework (If you do not have this installed the Policy Patrol program will download and install it for you).

If the above is installed, you can proceed with installing Policy Patrol as described in the 'Installation' paragraph. After the installation you will need to configure Policy Patrol as a mail gateway. If you only require Policy Patrol to process outbound mails (for instance if you have Policy Patrol Disclaimers and only want to add a disclaimer to sent messages), just follow the instructions in point (1). If you want Policy Patrol to process inbound as well as outbound mails, follow the instructions in points (1) and (2).

- (1) If you want Policy Patrol to process **outbound mails** you must forward all mail from the mail server to the Policy Patrol machine, and allow mail relaying from the mail server to the Policy Patrol machine:

- Forward mail from your mail server to the Policy Patrol machine:**

**If you have Exchange 2000:** On the Exchange 2000 machine open Exchange System Manager. Go to Servers > Exchange server name > Protocols > SMTP > Default SMTP virtual server > Properties > Delivery > Advanced. In the **Smart host** dialog box, enter the IP address in brackets, e.g. [192.168.2.200] of the Windows 2000 machine with Policy Patrol installed.

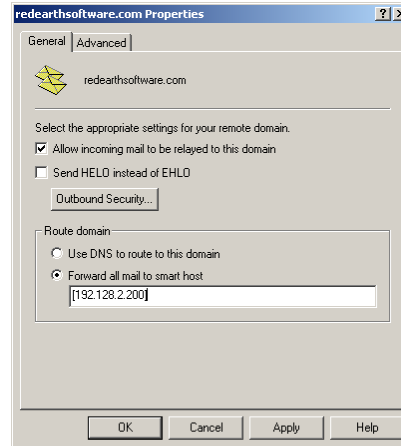
**If you have Exchange 5.5:** Open Exchange Administrator and go to Organization > Site > Configuration > Connections > Internet Mail Service Properties. In the Connections Tab go to the 'Message Delivery' section and in the dialog box **Forward all messages to host** enter the IP address of the Windows 2000 machine with Policy Patrol installed.

If you have **Lotus Domino R5/6 Mail Server:** Open Lotus Domino Administrator and select the server from which you wish to forward mail. Click on the **Configuration** tab. Go to Server > Configurations. Click **Edit Configuration**. Select the **Router/SMTP** tab and then the **Basics tab**. Enter the IP address of the Policy Patrol machine in **Local Internet domain smart host**.

- Allow mail relaying from the mail server to the Policy Patrol machine:** 1. On the Policy Patrol machine, go to Start > Settings > Control Panel > Administrative Tools > Internet Services Manager. 2. Right-click **Default SMTP Virtual Server** and select **Properties**. 3. Go to the **Access** tab and click on the **Relay** button. 4. Click **Add** and enter the internal IP address (can be the same as the external IP address) of the Exchange server machine in the single computer

dialog. 5. Click **OK** and stop and restart the Default SMTP Virtual Server (right-click > **Stop** and right-click **Start**).

- (2) If you want Policy Patrol to process **inbound mails** you must configure a remote domain in the Virtual SMTP Server on the Policy Patrol machine that will receive inbound mails and forward these to your mail server, and allow mail relaying from the Policy Patrol machine to your mail server:



- Create a remote domain and relay the mail to the mail server:** 1. On the Policy Patrol machine, go to Start > Settings > Control Panel > Administrative Tools > Internet Services Manager. 2. Go to **Default SMTP Virtual Server > Domains**. 3. Right-click **Domains** and select **New > Domain**. 4. The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**. 5. Enter the domain name, for instance `redearthsoftware.com`. Click **Finish**. 6. Select the newly created domain. Right-click and choose **Properties > General Tab**. 7. Tick **Allow incoming mail to be relayed to this domain**. In Route domain, select **Forward all mail to smart host** and enter the IP address of the mail server in between brackets, e.g. `[192.128.2.200]`. If you use multiple email domains, follow these steps for each domain.
- Allow mail relaying from the Policy Patrol machine to your mail server:** If you have Exchange 2000 follow the next steps: 1. On the mail server machine, go to Start > Settings > Control Panel > Administrative Tools > Internet Services Manager. 2. Right-click **Default SMTP Virtual Server** and select **Properties**. 3. Go to the **Access** tab and click on the **Relay** button. 4. Click **Add** and enter the internal IP address (can be the same as the external IP address) of the Policy Patrol machine in the single computer dialog. 5. Click **OK** and stop and restart the Default SMTP Virtual Server (right-click > **Stop** and right-click **Start**).

You are now ready to configure and start using Policy Patrol.



## Installation

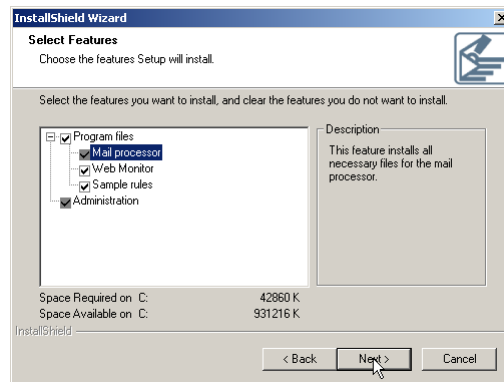
Follow the next steps to install Policy Patrol:

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the welcome screen, click **Next**.
3. Read the License Agreement and click **Yes** to accept the agreement.
4. Enter your user name and company name. If you want anyone who is logged on to the computer to be able to access Policy Patrol, select **Anyone who uses this computer (all users)**. If you only wish yourself to be able to access the program, select **Only for me (user name)**. Click **Next**.

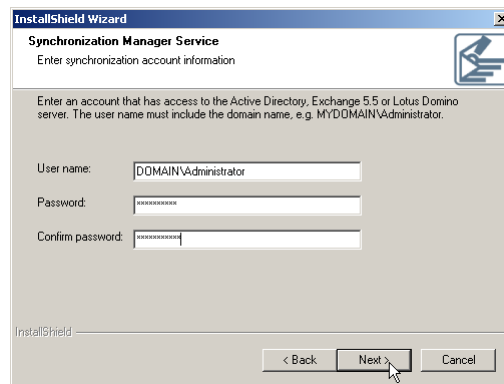
5. Select the setup type. If you select **complete**, the complete program will be installed in the default folder C:\Program Files\Red Earth Software\Policy Patrol. If you only wish to install the Administration console (for remote administration), select **Administration console**.

If you select custom, you will be able to change the location of the Policy Patrol folder and specify whether you wish to install the mail

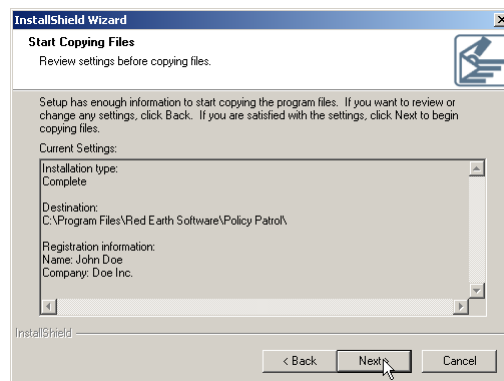
processor, Administration console, Web monitor and/or sample rules. Click **Next** to continue.



- Specify the user account that must be used for Synchronization. Make sure that this account has access rights to the Active Directory, Exchange 5.5 or Lotus Domino. Click **Next**.



- Review the installation settings. If they are correct, click **Next** to start copying files.



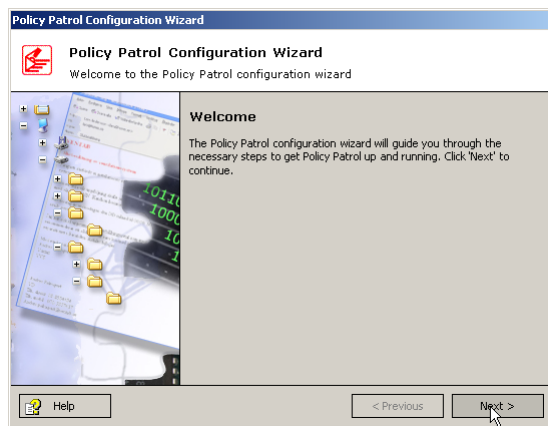
- When Policy Patrol has finished copying the files, the Policy Patrol Configuration wizard will start up. Continue to the next paragraph for

instructions on the Policy Patrol Configuration Wizard. When the configuration wizard has run, the Installation Wizard complete screen will pop up. Click **Finish** to exit the Installation wizard.

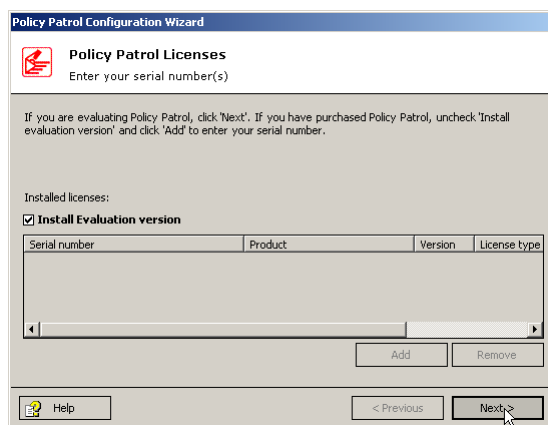
## Policy Patrol Configuration wizard

The Policy Patrol configuration wizard guides you through the necessary steps to get Policy Patrol up and running.

1. In the welcome screen, click **Next** to start the wizard.



2. If you are evaluating Policy Patrol, click **Next**. If you have purchased Policy Patrol, uncheck **Install evaluation version** and click **Add**. Enter your serial number and click **OK**. If you received your serial number via email, you can copy the serial number from your email and click on the 'Paste' button. Click **Next** to continue.



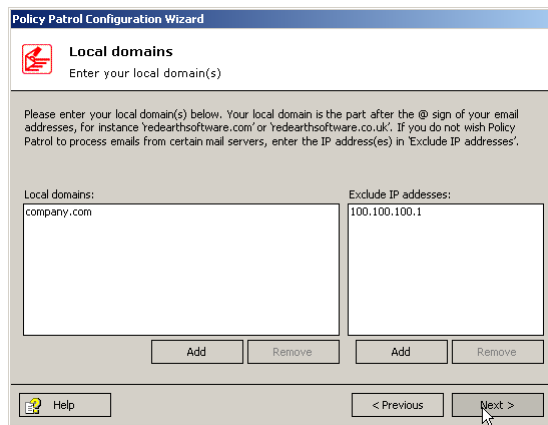
3. Enter your local domain(s). Your local domain is the part after the @ sign of your email address, for instance `redearthsoftware.com`. If you have installed Policy Patrol on the same machine as your mail server (only possible for Exchange 2000), Policy Patrol will retrieve your local

domains for you. To add a local domain, click on **Add**. Enter the domain, for instance `redearthsoftware.com`, and click **OK**. To remove a local domain, select the domain and click **Remove**.

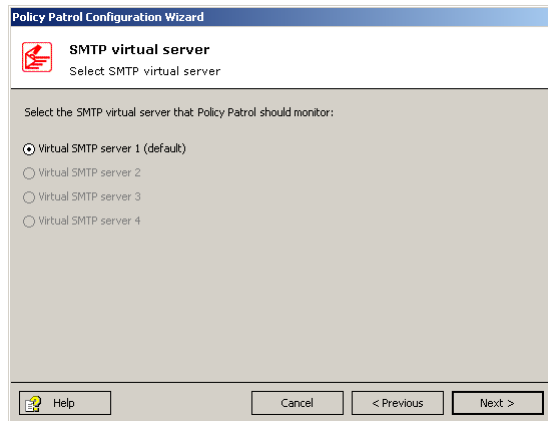
**i Info**

The local domains list is used to determine whether emails are internal or external. Emails that are sent from a local domain to a local domain are considered as internal, and emails sent from a local domain to a different domain and emails to a local domain from a different domain are considered external.

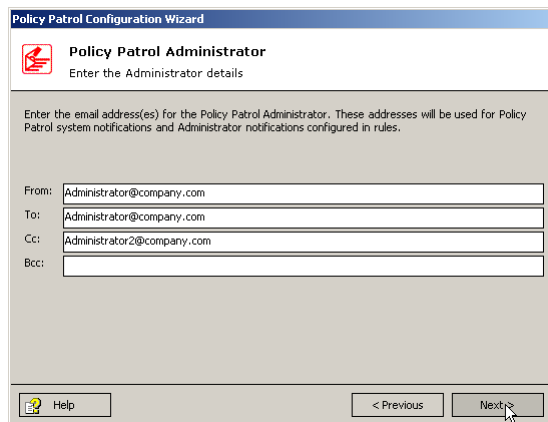
If you do not wish Policy Patrol to process emails from certain mail servers, enter the IP addresses in **Exclude IP addresses**. Click on **Add**, enter the IP address and click **OK**. When you are ready, click **Next**.



4. Select the virtual SMTP server that you wish Policy Patrol to monitor. If you only have one virtual server, the other options will be grayed out. Click **Next**.



5. Enter the email address(es) for the Policy Patrol Administrator. These addresses will be used for Policy Patrol system notifications and Administrator notifications configured in rules. You can enter a To:, Cc: and Bcc: email address. Remember that the From: field must include an existing, internal email address. Click **Next**.



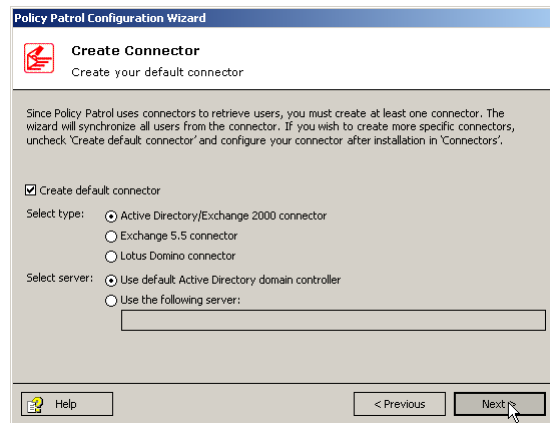
6. You must configure at least one connector so that Policy Patrol can retrieve your users. Select the type of connector you wish to create; **Active Directory/Exchange 2000, Exchange 5.5** or **Lotus Domino** connector. If you selected Active Directory, you can use the default Active Directory domain controller, or you can enter the name or IP address of another server. If you selected Exchange 5.5 or Lotus Domino you must enter the name of the mail server.

Policy Patrol will synchronize all users from the connector. If you wish to create a more specific connector, or if you wish to pick up users from a text file, uncheck **Create default connector**. You will then be able to configure your connector after installation in 'Connectors'. For instance, if you have a lot of users in your Active Directory and you only want to use Policy Patrol for selected users, it is better to create a more specific connector, rather than synchronizing all the users in your Active Directory. If you wish to use multiple connectors, for instance one

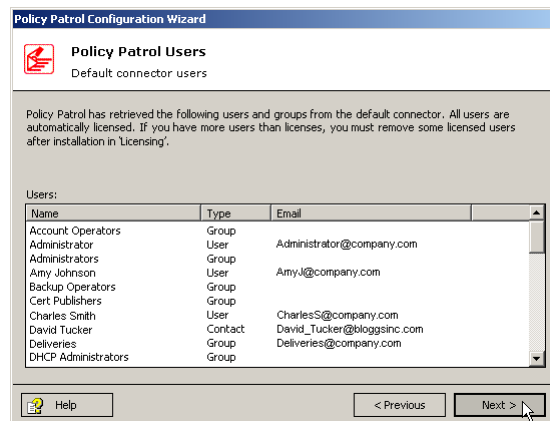
Exchange 2000 connector and one Lotus Domino connector, you can create the default connector during installation, and add more connectors in the Administration console after installation. When you are ready, click **Next**.

 **Note**

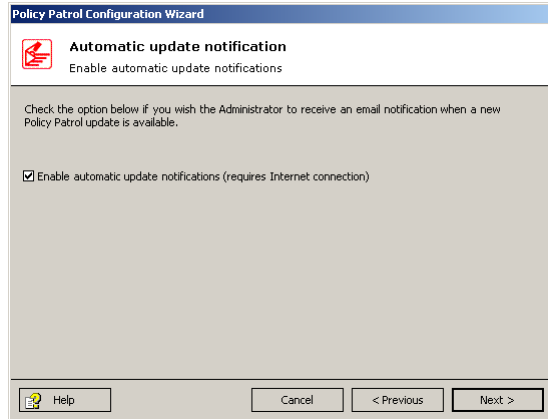
The Default connector is not **scheduled**. If you want Policy Patrol to automatically retrieve new users and updated user properties, you must configure scheduling of the Default connector after installation from **Connectors > Default connector > Properties > Schedule** tab.



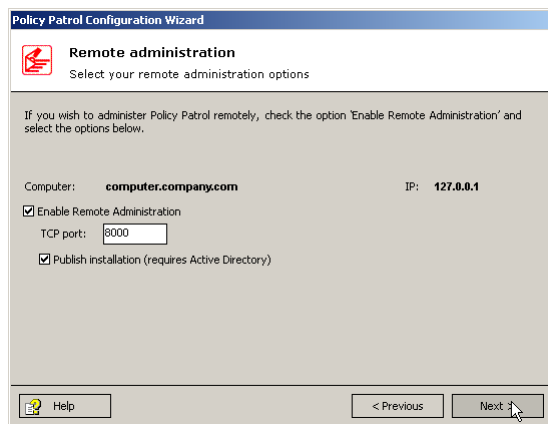
7. Policy Patrol will now display all the users from the default connector. All users will automatically be licensed. If you have more users than licenses, you must remove some licensed users after installation in 'Licensing', since otherwise Policy Patrol will select the licensed users randomly. Click **Next**.



8. If you wish the Administrator to receive an email notification when a new Policy Patrol update is available, check the option **Enable automatic update notifications**. In addition to an email notification, the Policy Patrol Update Wizard icon will appear in the system tray. Note that this option requires an Internet connection on the Policy Patrol machine.



9. If you wish to be able to administer Policy Patrol remotely, you must tick the check box **Enable Remote Administration**. Enter the TCP port to be used for connecting to the machine. By default 8000 is used. If you have multiple Policy Patrol installations that you wish to access remotely, each installation must use a different port. Select **Publish installation** to display the computer in a list that can be connected to from the remote machine. Note that this option is only possible if you have Active Directory.



10. Click **Finish** to exit the configuration wizard. You can now start configuring rules in the Policy Patrol Administration console. Go to Start > Programs > Policy Patrol > Administration. Select the computer name and choose **Connect**. The program already includes a number of sample rules. For more information on how to customize these rules,

consult the chapter 'Sample rules'. For more information on how to create your own rules, see chapter 'Configuring rules'.

 **Note**

Remember that after you make any changes in the Administration console, you must commit the changes by selecting server name > **Commit**, or by closing the Administration console and selecting 'Yes' when asked whether you wish to commit your changes. If do not commit, the settings are not saved. The server name will be followed by a \* if there are any changes that have not yet been committed, i.e. server name\*.

## Remote administration

If you wish to administer Policy Patrol from a remote machine, you can install only the Administration Console on the remote machine and connect to the server with Policy Patrol installed. If you have more than one Policy Patrol installation, you will be able to connect to each installation from the same machine. Requirements for the remote machine:

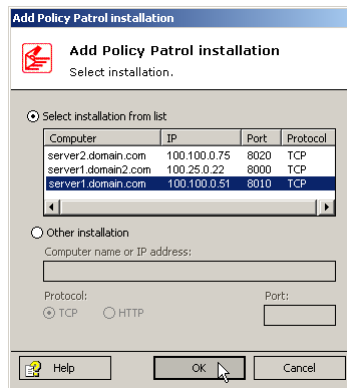
- Windows 2000 Professional or (Advanced) Server, or Windows XP Professional.
- Microsoft .NET Framework (If you do not have this installed the Policy Patrol program will download and install it for you).

To install remote administration:

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the welcome screen, click **Next**.
3. Read the License Agreement and click **Yes** to accept the agreement.
4. Enter your User name and Company name. If you want anyone who is logged on to the computer to be able to access Policy Patrol, select **Anyone who uses this computer (all users)**. If you only wish yourself to be able to access the program, select **Only for me (user name)**. Click **Next**.
5. Select **Administration console** as the setup type. Click **Next** to continue.



6. Review the installation settings. If they are correct, click **Next** to start copying files. When Policy Patrol has finished copying the files, the Installation Wizard complete screen will pop up. Click **Finish** to exit the Installation wizard.
7. Go to **Start > Programs > Policy Patrol > Administration**. The Policy Patrol Administration console will open up. Click on **Add installation**. If you have Active Directory and during installation of the main Policy Patrol program you selected to publish the installation, the computer name will show up in the list. Enable **Select installation from list**, and select the computer you want to remotely administer. If you do not have Active Directory or did not choose to publish the installation in the Active Directory, enable **Other installation**. Enter the Policy Patrol computer name or IP address, select **TCP** or **HTTP** and enter the **Port** number, for instance 8000. Remember that each Policy Patrol installation that you wish to administer remotely must use a different port number. Click **OK**. If you wish to administer multiple Policy Patrol installations, click on **Add installation** again and repeat the process.



8. To start administering Policy Patrol, click on the computer name and choose **Connect**.

## Creating Connectors

During installation Policy Patrol creates a default connector to retrieve your users. All users from the default connector are automatically synchronized and licensed. If you wish to pick up users from a text file, create more specific connectors or multiple connectors, you can do so from the Administration console. To create a new connector, follow the next steps:

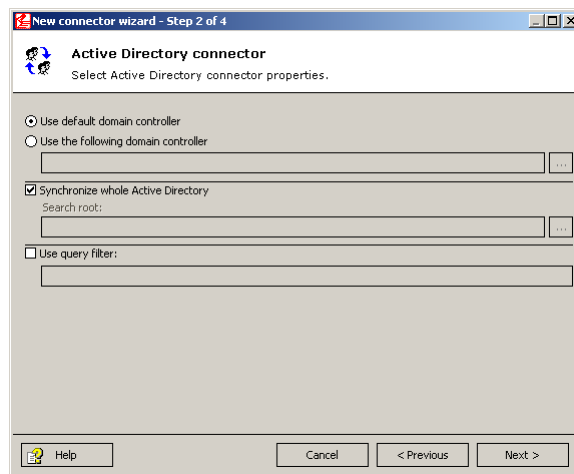
1. Go to **Connectors** and click **New....**
2. Select the connector type. If you have Exchange 2000 and/or Active Directory, select **Active Directory connector**. If you have Exchange 5.5, select **Exchange 5.5 connector**. If you have Lotus Domino, select **Lotus**

**Domino connector.** If you want to import users from a text file, select **Text file import connector**.

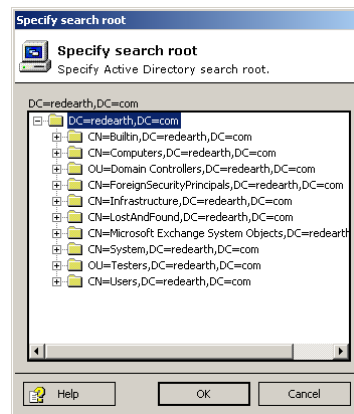
 **Note**

If you retrieve your users from Exchange 5.5, make sure that **LDAP** is enabled in Microsoft Exchange Administrator > Organization > Site > Configuration > Protocols > Properties > LDAP. Tick **Windows NT Challenge/Response** in the Authentication Tab and in the Search tab set the **Maximum number of search results returned** to at least 10.000.

3. **If you selected Active Directory Connector:** Leave the option **Use default domain controller** enabled, or if you wish to pick up users from another domain controller, select **Use the following domain controller** and click .... Now select the domain controller you wish to retrieve your users from and click **OK**. To pick up all users in the Active Directory, select **Synchronize whole Active Directory**.



If you only wish to pick up users from a certain Organizational Unit or group of users, uncheck **Synchronize whole Active Directory** and click on ... A dialog will open up. Now browse to the part of the Active Directory that you wish to synchronize with and click **OK**.



**If you selected Exchange 5.5 Connector:** Enter your Exchange server name or click ... to browse to the computer.

**If you selected Lotus Domino Connector:** Enter your Lotus Domino server name or click ... to browse to the computer.

#### **Note**

For the above connectors it is also possible to retrieve users that result from a query. To do this, enter the query string in **Query filter**. For instance, if you wish to create a connector with Active Directory contacts, you can enter (objectClass=contact) in the Query filter dialog box. For more information on how to enter the query, please send an email to [support@redearthsoftware.com](mailto:support@redearthsoftware.com).

**If you selected Text file import Connector:** Enter the path and file name to import the users from, e.g. C:\users.txt. The data in the text file must be entered as follows: First Name, Last Name, email address.

When you are ready, click **Next**.

4. Now select the scheduling for the connector. If you select **No scheduling** you will need to synchronize the connector manually each time you add new users and/or fields by selecting the respective Connector and choosing **Run now** in the Administration Console. To schedule the synchronization process and automatically update users and fields, select **Schedule this connector**. Choose hourly, daily, weekly or monthly synchronization. Click **Next**.
5. Enter the connector name and any comments for the connector. Select **Run connector on completion** to retrieve the users after you click **Finish**. Tick **License users automatically** if you wish to add all the synchronized users to the licensed users list. By ticking this option, new

users are automatically licensed in Policy Patrol upon synchronization. However you must make sure that you have enough Policy Patrol licenses since if this is not the case, Policy Patrol will randomly license your users.

 **Note**

The option **License users automatically** is only recommended if your Policy Patrol license covers all Connector users. If you select this option and have more users than licenses, Policy Patrol will randomly apply the available licenses to your users. Although you can then select which users should be licensed by going to **Licensing > Licensed users**, you would have to do this each time you run the connector.

## Licensing

Policy Patrol is available in two versions, Policy Patrol Disclaimers and Policy Patrol Enterprise.

### Policy Patrol Disclaimers

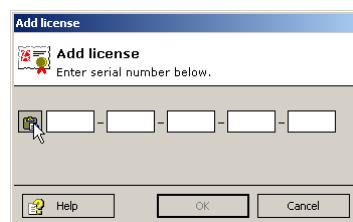
This version only provides the disclaimer functionality, which effectively means that when creating rules, only the **Accept**, **Add disclaimer**, **Send blind copy** and **Replace words/phrases in subject** actions are available. Moreover, the tree nodes **Archiving**, **Reporting**, **Monitoring**, **Anti-virus** and **Spam blocker** will be removed. All conditions, exceptions, filters and disclaimer templates will still be available though.

### Policy Patrol Enterprise

This version includes all Policy Patrol features, including disclaimers and anti-virus.

## Add license

To add your serial number, go to **Licensing**. In 'Installed Licenses', click **Add**. Now enter your serial number. If you have received your serial number via email, you can copy it and click on the 'Paste' button. The number will automatically be pasted into the dialog. Click **OK** to add the license.



## Licensed users

Policy Patrol allows you to only license the users that you wish to create rules for. When you create a connector, you can select to license all users. However, if you only wish to license certain users you can do this from **Licensing > Licensed users**. The dialog will show a list of licensed users. To add more users, click **Add**. The list will show all users that were synchronized from your configured connector(s) less the users already licensed. Select the users to add and click **OK**. To remove licensed users from the list, select the user(s) and choose **Delete**. The number of available licenses will be shown in the top right corner.

### Note

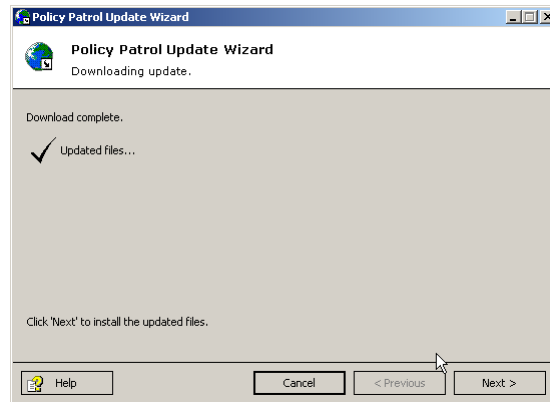
If you have more users than licenses, the available licenses will be in red and will include a minus, for instance **Available licenses: -20**. If you don't remove the over licensed users from the licensed user list, Policy Patrol will randomly select licensed users each time a mail is sent. As soon as you over license users, the Administrator will receive a notification email and there will be a warning in the System events.

## Policy Patrol Update Wizard

Policy Patrol includes an update wizard that allows you to automatically download and install updates without losing your configuration. During installation you can select whether you wish the update wizard to automatically check for new updates. If enabled, the Policy Patrol Update Manager service will check for new updates once a day. If the update manager finds a new update, the update wizard icon will appear in the system tray of the Policy Patrol machine, and the Administrator will receive an email notification about the new update.

To apply a new update, or manually check for new updates:

1. Right-click on the Update Wizard icon in the System Tray and choose **Run update wizard**, or go to **Start > Programs > Policy Patrol > Update Wizard**. The update wizard will start up.
2. In the Welcome screen, click **Next**.
3. Wait whilst Policy Patrol checks if there are any updates available and downloads the relevant information. The information will include a description of the update and a list of fixes and new features (if any). When ready, click **Next** to download the update.



4. Policy Patrol will now download the update. When the download is complete, click **Next** to install the update.
5. Wait whilst Policy Patrol applies the update. If any services need to be restarted, a dialog will pop up warning you about this. When Policy Patrol is ready, click **Finish** to exit the update wizard. You now have the latest version of Policy Patrol installed.

#### **Note**

Remember that you must run the update wizard on each Policy Patrol machine. For instance, if you have a remote installation of Policy Patrol you must run the update wizard on both the local machine as well as the remote machine.

## Services

You can stop and start the Policy Patrol services by clicking on your server name and selecting the following services:

- ✓ SMTP sink (if you stop this service, Policy Patrol will not filter any mails but messages will still get delivered)
- ✓ Mail Processor (if you stop this service **no mails will be delivered** and all mails will end up in the queue directory)
- ✓ Remote Administration Manager (this service enables remote administration)
- ✓ Synchronization Manager (this service runs connectors at scheduled times)

## INSTALLING POLICY PATROL

- ✓ Update Manager (this service checks for new updates)

To start a service, select the service and click on the **Start** button. To stop a service, select it and click **Stop**.

## Configuring rules

**I**n addition to the sample rules included in the program, Policy Patrol includes the possibility to configure your own customized rules. This chapter describes how to configure rules in Policy Patrol.

### Configuring a new rule

To configure a new rule, go to **Policy rules** and click on the **New...** button. The rules wizard will appear. The wizard window is divided into two panes. The rule options are displayed in the top pane. Each time you select an option, a description of it is placed in the bottom pane. If you still need to set a certain value, the description will include a **red link**. Click on this link to configure the respective option. Once a value is set, the link color will change to **blue**. A selected link will appear in **purple and underlined**. If you have not yet set all values when you click finish to create your rule, a warning will pop up. You will still be able to create the rule, but the rule will not be enabled until you set all values.

The rules wizard will guide you through the following steps:

#### **Step 1. Which users should this rule apply to?**

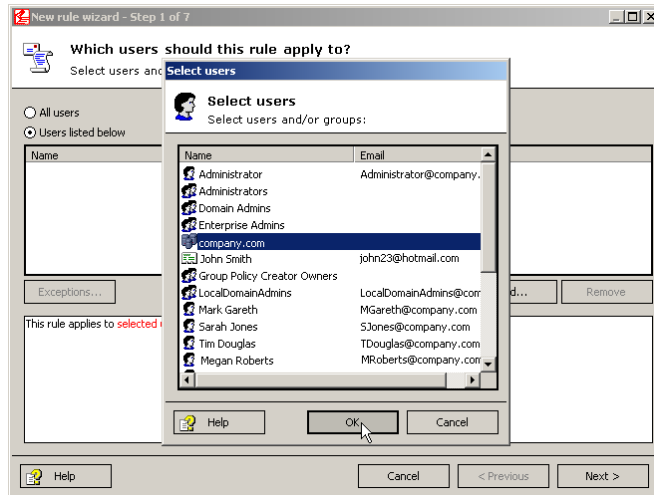
To apply the rule globally, select **All users**. To apply the rule to certain users, groups, public folders or domains (see note below) select **Users listed below** and click **Add...** Select the users for the rule and click **OK**. If you wish to add exceptions, for instance if you wish the rule to apply to all users apart from the Board of Directors, click on **Exceptions...** and **Add...** Select the user to exclude, click **OK** and **Close**. Click **Next**.

#### **Note**

Policy Patrol includes the option to select domains when configuring rules. To add domains to the user list, go to server name > Properties > Advanced tab. Click on **Add** and enter SYNC\_ADD\_DOMAIN\_ADDRESSES and enter 1 as the value. Click **OK**. Commit the changes and run the respective



Connector(s). When selecting the users for a rule, you will now also be able to select domains in the list.

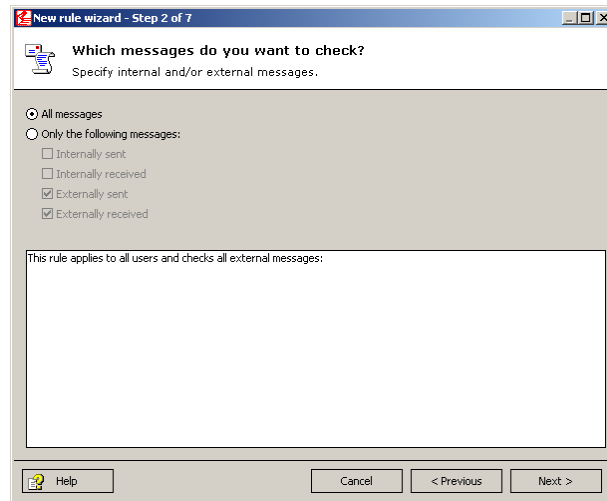


**Tip**

If you wish to create a rule that applies to Active Directory contacts, you can apply the rule to all users and then specify the condition that the To: or From field should contain an address from a filter that retrieves your contacts from a connector. For more information on how to create such a filter, consult the paragraph ‘Creating a Domain/Email Address Filter’ in the chapter ‘Creating Filters’.

**Step 2. Which messages do you want to check?**

Specify whether you wish to check all messages or only internally sent and/or received messages, and/or externally sent and/or received messages. Remember that Policy Patrol can only check internal messages if you have installed Policy Patrol on an Exchange 2000 machine. Click **Next**.

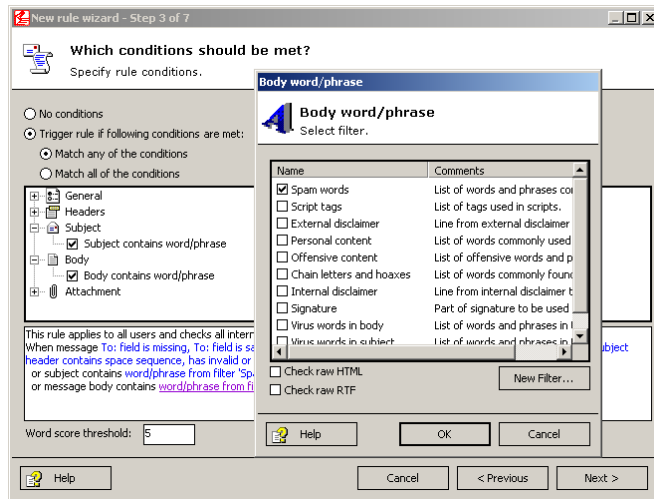


### Step 3. Which conditions should be met?

Here you must specify which conditions should be met for the rule to trigger. If the rule should always trigger (for instance if you want to archive all messages), leave **No conditions** selected and click **Next**. If the rule should only trigger in certain circumstances, select **Trigger rule if following conditions are met**. The different conditions are sorted into 5 categories: General, Headers, Subject, Body and Attachment.


If any of the conditions must be met, select **Match any of the conditions**. For instance, if you wish to block spam mails and want to create a rule that deletes messages that either contain words from the spam filter or originate from domains on a spam list, select this option. If all the conditions must be met, select **Match all of the conditions**. Select this option if, for instance, you wish to add high priority to messages from an important customer email address/domain list with 'urgent' in the message.

If you select a word/phrase condition, the **Word score threshold** box will become active. Here you must enter the total word score for the email message. If the email reaches the word score threshold, the rule will trigger. For instance, if the email message contains the phrase 'CLICK HERE', which is attributed a word score of 5 and the rule has a word score threshold of 5, the rule will be triggered. By setting different word scores and applying negative scores for certain words, it is possible to closely identify the content of emails and in doing so greatly decrease the occurrence of false positives (i.e. wrongly triggered rules). For instance, you might want to apply a word score of 5 to the word 'breast', but would like to set a negative score if in the same message the word 'baby' or 'milk' is found. Then you could apply a -2 score for both words and set the word score threshold to 5. More information on how to apply word scores can be found in the chapter 'Creating Filters'.



If you specify more than one word/phrase filter to content check, Policy Patrol will add the scores of all words/phrases and trigger the rule once the word score threshold is reached. Similarly, if you select to check word/phrase filters for subject, body and/or attachment, Policy Patrol will add all the scores and trigger once the total score reaches the word score threshold.

If you do not use the word score option in your word/phrase filters, leave the threshold set to '0'. The rule will then trigger when any word/phrase from the filter is found. If you configure a rule that checks multiple word/phrase filters, some with and some without word score enabled, Policy Patrol will trigger the rule if words/phrases from the word score filter reach the word score threshold, or if any word/phrase from the non-word score filter is found in the email.

 **Note**

If you select to check a word/phrase filter with word score enabled and leave the word score threshold set to '0', the rule will always trigger since every message will reach the word score threshold of '0'.

Available conditions:

- **General**
  - Message is encrypted:** This condition checks whether a message is encrypted. You can further distinguish between S/MIME and PGP encrypted messages.
  - Message is digitally signed:** This condition checks whether a message is digitally signed. You can further distinguish between S/MIME and PGP digitally signed messages.

- ❑ **Message is of size:** Specify whether the message size (this includes headers, message text and attachments) should be greater than, less than, between or not between certain values. If you select **Greater than** or **Less than**, the value you enter will not be included, e.g. if you select greater than 1 MB, the rule will trigger on a message of 1.1 MB, but not on 1 MB. If you choose **Between** or **Not between**, the values you enter will be inclusive, e.g. if you specify that the message size should be between 2 and 3 MB, the rule will trigger for messages of 2 MB and 3 MB and any size in between. If you select not between 2 and 3 MB, the rule will not trigger for messages of 2 MB and 3 MB and any size in between.

 **Note**

Policy Patrol counts the actual message size as received by the mail server. This can be a little different from the message size as received by Outlook or the message size of a Quarantined message in Policy Patrol. There are a number of reasons for this, such as different encoding of the email or attachment, or the method of determining the size, e.g. storage space or bandwidth used.

- ❑ **Message is of date:** Specify whether the message date must be equal, after, before, between or not between certain dates. If you select **before** or **after**, the date itself will not be included. For instance, if you specify that a rule should trigger for dates before October 1st, the rule will trigger for messages sent on or before September 30<sup>th</sup>, but not on October 1<sup>st</sup>. If you select **between** or **not between**, this will include the two values. For instance, if you select **between** 5<sup>th</sup> and 7<sup>th</sup> September, the rule will trigger for messages sent on 5<sup>th</sup>, 6<sup>th</sup> and 7<sup>th</sup> September. If you select **not between** 5<sup>th</sup> and 7<sup>th</sup> September, the rule will not trigger for messages sent on 5<sup>th</sup>, 6<sup>th</sup> and 7<sup>th</sup> September.
- ❑ **Message is of priority/importance level:** Specify whether the message should be of High, Normal and/or Low priority.
- ❑ **Message is of sensitivity level:** Specify whether the messages should be Normal, Personal, Private and/or Confidential.

 **Note**

The sensitivity level only applies to internal messages sent from Microsoft Outlook. If a message with a certain sensitivity level

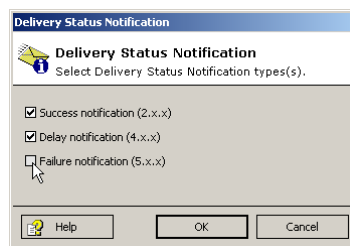
is sent or received externally, this email attribute is lost and cannot be checked by Policy Patrol.

- ❑ **Message contains delivery receipt request:** By checking this option Policy Patrol will check if the message contains a delivery receipt request. There are no further options for this condition.
- ❑ **Message contains read receipt request:** By checking this option Policy Patrol will check if the message contains a read receipt request. There are no further options for this condition.
- ❑ **Message is of format:** Specify whether the message should be of plain text, HTML and/or rich text format.

 **Note**

Remember that when sending externally from Exchange server it depends on your settings whether the mail is sent as rich text or HTML. By default all external mail is either sent in plain text, or HTML & plain text since otherwise other clients may not be able to view the message.

- ❑ **Message is Delivery Status Notification:** Specify whether the message should be a Success, Delay and/or Failure notification. If you wish to filter Delivery Status Notifications (DSNs), you must select to check externally sent and/or internally sent messages in step 2 of the Rules Wizard. The user of the rule must be the postmaster.



 **Note**

If you select this condition, make sure that you license the postmaster email account since the postmaster is the sender of a DSN.

 **Tip**

You can use this condition to block **Non-deliverable Report Spam attacks**. An NDR 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 (failure DSN) to the sender, i.e. the spam victim, with the original spam message attached. In Exchange server there is no way to stop non-deliverable messages from being sent. However, in Policy Patrol you can delete or quarantine externally sent non-deliverable messages. For more information on how to do this, please consult the Policy Patrol knowledge base at <http://www.policypatrol.com>.

- ❑ **Message contains virus:** By checking this option the rule will trigger for messages that contain a virus. You can select to check for messages that contain a virus that has been cleaned, a virus that could not be cleaned, a virus that has been deleted, a virus that could not be deleted or a suspected virus.

Policy Patrol can try to clean viruses in all messages, and for external messages delete the infected part if the virus could not be cleaned (These settings are configured in **Anti virus**). However, Policy Patrol cannot delete the infected part of an internal message without deleting the entire message. Therefore you must always include a rule that specifies what should be done with internal messages that contain a virus that could not be deleted. In exceptional circumstances it is also possible that Policy Patrol cannot delete a virus from an external message. Therefore it is recommended to configure a rule that specifies to for instance delete or quarantine all messages that contain a virus that could not be deleted.

Suspected viruses include scripts or code that are not known viruses, but are identified by Kaspersky™ Anti-Virus as potentially harmful. This category also includes messages that could not be scanned, for instance password protected attachments.

 **Tip**

It is advisable to activate the sample rule **Quarantine viruses that could not be deleted**, since otherwise the occasional virus could still get through.

- **Headers**

- **Sender field contains domain or email address:** Select the filter of email addresses and/or domains that must be present in the From: field. If you wish to make a new filter for this rule, click **New Filter...** This condition will only apply to received messages. If you are only checking sent messages, this condition will not be available.

 **Note**

This option is grayed out if you have specified to check only sent messages, since by selecting the users for the rule, you have already specified which email address should be listed in the From: field. If you check both sent and received messages, this field will be available but will only apply to received messages.

- **Receiver fields contain domain or email address:** Select the filter of email addresses and/or domains that must be present in the receiver fields. The receiver fields include the To:, Cc:, Bcc: and X-Receiver fields and means that all recipients of the mail will be checked. If you wish to make a new filter for this rule, click **New Filter**. This condition will only apply to sent messages. If you are only checking received messages, this condition will not be available.
- **Receiver fields contain number of recipients:** Specify whether the number of recipients in the To: and Cc: field should be **More than**, **Less than**, **Between** or **Not between** a certain value. If you select **More than** or **Less than**, the value itself will not be included. For instance, if you specify that a rule should trigger when there are **More than** 2 recipients, the rule will trigger for messages with 3 or more recipients. If you select **Between** or **Not between**, this will include the two values. For instance, if you select **Between** 2 and 4 recipients, the rule will trigger for messages with 2, 3 and 4 recipients. If you select **Not between** 2 and 4 recipients, the rule will not trigger for messages with 2, 3 and 4 recipients. Policy Patrol cannot count bcc: recipients. Distribution lists will be counted as one recipient. This condition will only apply to sent messages. If you are only checking received messages, this condition will not be available.

**Note**

These options are grayed out if you have specified to check only received messages, since by selecting the users for the rule, you have already specified which email address should be listed in the To: field. If you check both sent and received messages, this field will be available but will only apply to sent messages.

- ❑ **Header of name and value exists:** Enter the header name and value. For instance, you could search for the header `X-Mailer` and enter a number of Mail Delivery Agents that are frequently used by spammers. Note that you must enter the `x-` in front as well, so for instance if you wish to search for the header `X-SPAMHAUS`, you must enter `X-SPAMHAUS`. Some spam messages include a Precedence field, of which the value is `bulk`. To check for this condition, enter `Precedence` and enter `bulk` as the value.

Name	Value
X-SPAMHAUS	TRUE
Precedence	bulk

- ❑ **Header contains spam characteristics:** Select the different spam characteristics that Policy Patrol must check for. By analyzing several different spam messages, Red Earth Software has been able to identify the most commonly found spam headers and has included them in this list. For more information on the background of spam characteristics, read the article 'How to effectively block spam and junk mail' at: <http://www.redearthsoftware.com/spam-filter-article.htm>.

**To: field is missing, empty or of an invalid format:** Because spammers send out bulk emails by entering all recipients in the Bcc: field or X-Receiver header, the To: field of spam mails is often missing, empty or of an invalid format. Check this option to block these messages.

**To: field is same as From: field:** This is usually a characteristic of a mailing where all recipients are in the bcc: field. Instead of



entering one email address in the To: field, the sender adds their own email address in the To: field. Check this option to catch spam as well as personal mailings.

**From: field is missing or empty:** Spammers remove the From: address in an attempt to disguise the sender. This characteristic is a sure sign of spam.

**Bcc: field exists and is empty:** In genuine email messages, a Bcc: header does not exist since this is stripped from the mail. Therefore, the existence of a bcc: field indicates a bulk mailing.

**Subject header is missing:** Some spammers do not use a subject. However, this option could cause false positives since it will also catch genuine messages without a subject.

**Subject header contains space sequence:** Many spam mails include a certain code for identification in the subject of the message. To hide the code from the recipient, a large number of spaces are usually placed before the code. This is done so that the recipient won't notice the code or that it is not displayed in the mail client. Since there is no genuine reason to include many spaces in the subject, this characteristic is a sure sign of spam.

**Invalid or missing Message ID:** Since the Message ID includes information about where the message comes from, it is often missing or malformed (i.e. no @ sign or an empty string) in spam messages.

**X-UIDL header exists:** Incoming messages should not have an X-UIDL header since they are only intended for the mail server to stop it downloading messages more than once, for instance when 'leave messages on server' is checked. This header would normally be stripped when the message is received. Spammers add an X-UIDL header to try to get the recipient's mail server to download multiple copies of their message and therefore increase the chance that the message will be read.

**Message contains illegal HTML:** Some spam messages include a code for identification in the text of the message. The text is entered outside the HTML tags so as to hide the code from the recipient. There is no reason to add text outside HTML tags, so the mere presence of illegal HTML can be treated as suspicious.

- **Subject**

- **Subject contains word/phrase:** Select the word/phrase filter that Policy Patrol must check for in the subject of the message. If you wish to create a new filter for the rule, click **New Filter...**

- **Body**

- **Body contains word/phrase:** Select the word/phrase filter that Policy Patrol must check for in the body of the message. If you wish to check the HTML source code, check the option **Check raw HTML**. This can be useful if you want to check for scripts by searching for the `<SCRIPT>` tag. If you want to check for RTF tags, you must select **Check raw RTF**. If you wish to create a new filter for the rule, click **New Filter...**

 **Note**

When checking for words/phrases remember that if word score is enabled, which it is by default, you must enter a word score threshold when configuring the rule. If you leave the threshold set to 0, the rule will trigger for every message.

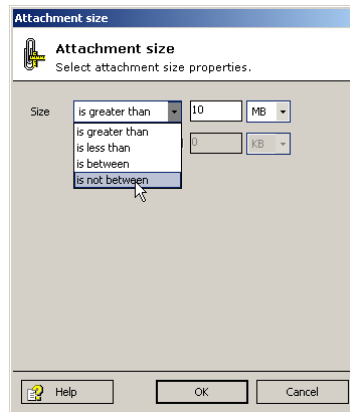
- **Attachment**

- **Attachment exists:** By checking this option Policy Patrol will check if the message contains an attachment. There are no further options for this condition.

 **Note**

By default, inline HTML pictures are counted as an attachment. If you do not wish inline HTML pictures to be counted as attachments, you can change this by adding a system parameter. Please contact [support@redearthsoftware.com](mailto:support@redearthsoftware.com) for instructions on how to do this.

- **Attachment is of size:** Specify whether the attachment should be **Greater than**, **Less than**, **Between** or **Not between** certain values. Each attachment to the message is counted separately. So if you have a rule that triggers when an attachment is greater than 1 MB, the rule will not trigger for a message that includes two attachments of 550 KB each. If you wish to create such a condition, you can use the Message size property in the General conditions instead.



- ❑ **Attachment is of type:** Select the attachment type filter Policy Patrol must check for. If you wish to create a new filter for the rule, click **New Filter...**
- ❑ **Attachment is of name:** Select the attachment name filter Policy Patrol must check for. If you wish to create a new filter for the rule, click **New Filter**.
- ❑ **Attachment contains word/phrase:** Select the word/phrase filter Policy Patrol must check for. Policy Patrol can check text, html and Microsoft Word documents for words. If you wish to content check Microsoft Word documents, you must select **Enable Microsoft Word content checking** in Computer name > **Properties** > **Attachment checking** tab and install Microsoft Office XP (Word only) on the Policy Patrol server machine. If you wish to check the HTML source code of an html file, check the option **Check raw HTML**. This can be useful if you want to check for scripts in attachments, for instance by searching for the <SCRIPT> tag.
- ❑ **Attachment is spoofed:** By checking this condition Policy Patrol will check whether the attachment has been changed to disguise the actual file format. You can select four options:

**Check for multiple extensions:** Sometimes files that contain viruses are given double extensions, for instance `virus.txt.exe`. This is done because Outlook will only show the first extension, fooling recipients into thinking that the file is a text file instead of an exe file. If you check this option, Policy Patrol will check for files with multiple extensions.

**Check for CLSID extension:** Some viruses are spread by giving files CLSID extensions. This makes the file seem to be of a different or unknown file format, but when opened will activate a predetermined application. For instance, a virus executable could be named `virus.txt` and given a CLSID extension. This will make the

file look like a txt file (although the icon will be for an unknown file format). However, when the user double-clicks on the file the program will execute. If you tick this option, Policy Patrol will check for files that have been given a CSLID extension.

**Check for binary text file:** Some files might be disguised as text files to avoid filters blocking the message. For instance, pictures could be renamed as a .txt file. In this case the text files will not contain text, but binary code. By checking this option, Policy Patrol will check whether text files contain binary code.

**Attempt to verify attachment extension:** Policy Patrol can verify over a 100 file types. A list of files that Policy Patrol can verify is found in server name > **Properties** > **Attachment Spoofing**. For instance, if a user tries to circumvent a rule blocking exe files and renames the `virus.exe` file to `virus.doc`, Policy Patrol will block this file since it can verify that the file is not a doc file.

- ❑ **Message contains number of attachments:** Specify whether the number of attachments must be **More than**, **Less than**, **Between** or **Not between** a certain value. If you select **More than** or **Less than**, the value itself will not be included. For instance, if you specify that a rule should trigger when there are **More than 2** attachments, the rule will trigger for messages with 3 or more attachments. If you select **Between** or **Not between**, this will include the two values. For instance, if you select **Between 2 and 4**, the rule will trigger for messages with 2, 3 and 4 attachments. If you select **Not between 2 and 4**, the rule will not trigger for messages with 2, 3 and 4 attachments.

#### **Note**

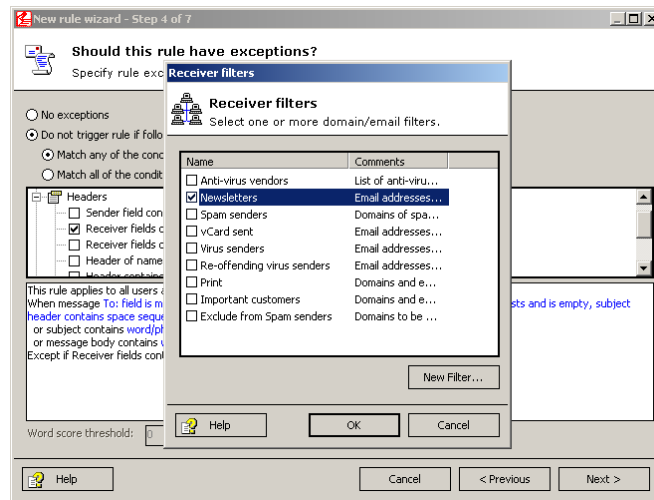
By default, inline HTML pictures are counted as an attachment. If you do not wish inline HTML pictures to be counted as attachments, you can change this by adding a system parameter. For instructions on how to do this, please consult [support@redearthsoftware.com](mailto:support@redearthsoftware.com).

When you are ready specifying the conditions to be met, click **Next**.

#### **Step 4. Should this rule have exceptions?**

If the rule has no exceptions, leave the option **No exceptions** enabled. To specify exceptions, activate **Do not trigger rule if following exceptions are met**. The options will now be the same as in step 3. Exceptions can for instance be useful for using 'white lists'. An example of a white list is a Domain/Email address filter that contains the addresses of allowed newsletters.

Messages originating from these addresses could for instance be excluded from a spam rule. When you are ready specifying the exceptions, click **Next**.



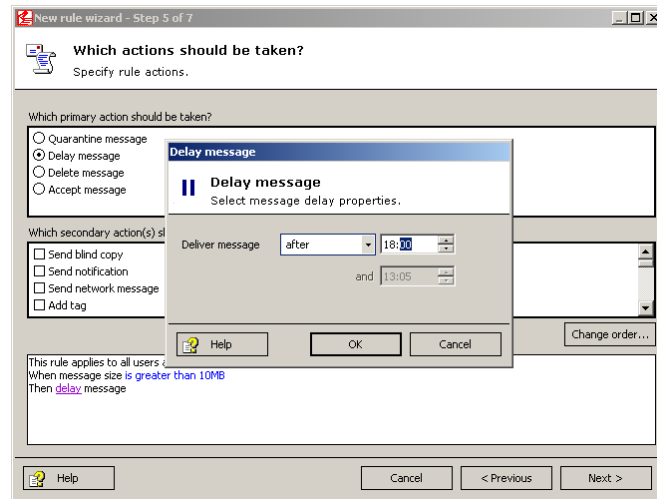
**Step 5. What actions should be taken?**

Policy Patrol includes two different types of actions: primary and secondary actions. The primary actions are mutually exclusive, i.e. you can only choose one primary action. After you select a primary action, you will be able to select secondary actions. You can select as many secondary actions as you wish.

**Primary actions**

You have the choice out of four primary actions:

1. **Quarantine message:** This option will hold the mail in quarantine until the message is accepted or rejected. When you select this option, the action will appear as **quarantine message (don't send approve/reject notification)** including a blue link in the bottom window. Approve/reject notifications are sent when the message is either accepted or rejected and can include remarks from the moderator. If you do not want to send any accept/reject notifications, you do not need to configure this option any further. If you want to add accept/reject notifications, click on the quarantine link. You can specify an approve/reject notification for the sender, recipient, their managers, the Administrator, or any other email address. For more information on how to accept and reject quarantined messages, consult the chapter 'Monitoring messages'.
2. **Delay message:** This option will delay the message for delivery at a later time. After you select to delay the message, click on the **delay** link and specify whether the message should be delivered **After**, **Between** or **Not between** certain times. For more information on how to view and deliver delayed messages before the specified time, consult the chapter 'Monitoring messages'.



3. **Delete message:** This option will delete the message (you will still be able to undelete the message from **Monitoring > Deleted**).
4. **Accept message:** This option will let the message pass through as normal.

**Secondary actions**

The following secondary actions are available:

- ❑ **Send blind copy:** Select this option to send a blind copy of the message. You can use this option to save messages to a certain mailbox for monitoring or backup purposes. Click on the **send blind copy** link and enter the email address to send the copy to. Alternatively, click on the ... button and select the user(s) or group(s) from the list. You can also select to send a copy to the sender's or recipient's manager.

Only if you have Exchange 2000: if you want to send a copy of an internal message to an external recipient, you must tick the option **Convert TNEF encoded message to plain text**. If you do not tick this option, the external recipient will not be able to view the message since it will be encoded in Microsoft Exchange server proprietary format.

- ❑ **Send notification:** By selecting this option, Policy Patrol will send a notification message. In the options, specify who should receive the notification (recipient, sender, administrator, manager, or other) and select the template to be used for each recipient. If you wish to use a new template, click **New Template....**

 **Note**

The manager's email address will be taken from the Active Directory user properties. If the sender or recipient is external, no

notification is sent since the manager of an external recipient is not known. The Administrator address(es) are taken from server name > Properties > System notifications tab.

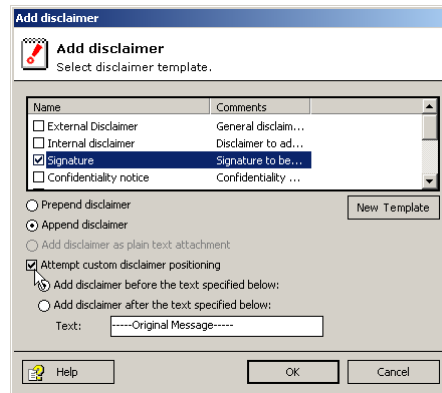
#### **Tip**

Policy Patrol notification messages include the custom header `x-policypatrol:notification` for easy identification. For instance, this enables you to place all Policy Patrol notification messages in a separate Outlook folder by creating a rule in Outlook that triggers when this header is found.

- ❑ **Send network message:** In the **To** field enter the user name or IP address of the computer you wish to send a network message to. In **Tag**, select the message to be sent by choosing a tag from the drop down box.
- ❑ **Add tag:** This option allows you to add a tag to the message. For instance, as a warning to users you could add the tag `'CAUTION: POSSIBLE VIRUS'`. You can add a tag to the subject or archive. If you choose to add a tag to the subject, you can select to prepend or append the tag. If you prepend the tag, it will appear before the subject as follows: `[Tag]Original subject`. If you choose to append the tag, it will appear after the subject as follows: `Original subject[Tag]`.

You can also add a tag to an archive. For instance you might want to flag spam messages or messages with viruses. To specify which tag to add, select the tag template and the archive to be used. If you wish to create a new template or archive, click on the **New Template** and **New Archive** respectively.

- ❑ **Add disclaimer(s):** This option will add a disclaimer or signature to the message. In the options, select the disclaimer template from the list and specify whether you wish to append, prepend or attach it as a text file. If you wish the disclaimer or signature to be placed within the message, select **Attempt custom disclaimer positioning**. This can be useful for signatures, so that when replying or forwarding they get placed after your last message text, not completely at the bottom of the email. Select **Add disclaimer before the text specified below**, or **Add disclaimer after the text specified below**. By default the text dialog contains the line that appears when replying or forwarding from Microsoft Outlook. However, you can alter the text if necessary. If the disclaimer-positioning attempt fails, for instance if the specified text cannot be found, Policy Patrol will prepend or append the disclaimer/signature, depending on the option you selected.



You can select multiple disclaimers if you wish. Remember that if you select **Add disclaimer as plain text attachment**, the disclaimer text must be entered in the RTF/plain text tab of the Disclaimer template. If there is only text entered in the HTML tab, the attachment will be empty. If you wish to create a new disclaimer, click **New Template**.

- ❑ **Add attachment(s)**: This option adds an attachment to the original message. Click on the **add attachment(s)** link and click **Add**. Browse to the attachment and click **Select**. Click **OK** to close the dialog.
- ❑ **Remove attachment(s)**: This option will remove all attachments from the message. There are no further options for this action. Note that pictures in HTML messages also count as attachments, so if you select this option all HTML pictures will be removed as well.

 **Note**

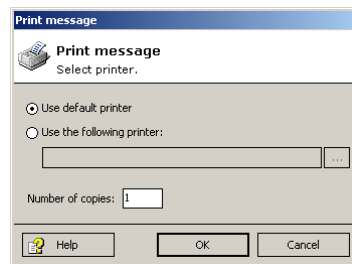
By default, inline HTML pictures are seen as attachments and are therefore stripped if you select **Remove attachment**. If you do not wish inline HTML pictures to be counted as attachments, you can change this by adding a system parameter. Please contact [support@redearthsoftware.com](mailto:support@redearthsoftware.com) for instructions on how to do this.

- ❑ **Compress attachment(s)**: Use this option to automatically compress attachment(s). Click on the **compress** link and specify the compression options. Select whether you wish to **Create one archive for all attachments**, or **Create one archive for each attachment**. If you wish to create one archive, you must specify a name to be used, for instance `Attachments.zip`. In compression type, select **Maximum** (maximum compression but slowest to process), **Default** (medium compression, reasonably fast to process) or **None** (no compression, simply store in archive file). In the Options, you can select a tag to be added as an archive comment. This comment will appear when the user



opens the archive file. Note that only externally sent or received attachments can be compressed and that zip files are automatically excluded from the compression action.

- ❑ **Decompress attachment(s):** Use this option to automatically decompress attachment(s). Click on the **decompress** link and specify the decompression options. Select **Decompress all zip attachments**, or **Do not decompress if extracted file(s) are greater than, less than, between, not between** certain values. If you wish to decompress zip files that have been zipped, select the option **Decompress archives within archives**. Note that only externally sent or received zip files can be decompressed.
- ❑ **Add business card (vCard):** If you select this option the business card of the sender will be added to the mail. This option is only applicable to internal messages and externally sent messages.
- ❑ **Print message:** This option will print out a copy of the message. This can be useful for legal companies that are obliged to print out copies of emails. It might also be useful for certain sent and/or received mails. In the options, specify the printer and the number of copies to be printed. The email will be printed in plain text, including the attachment file name(s) if any.



- ❑ **Replace words/phrases in subject:** Select this option to replace a word or phrase in the subject. Enter the words or phrases to be replaced in the 'Word/phrase' column, and in 'Replace with' enter the new text to be entered. If you wish the text to be removed, simply leave the 'Replace with' column blank. By ticking the case sensitive option, Policy Patrol will only replace the words if they are in the same case as entered in the Word/phrase column.

 **Tip**

This function can be used if you wish to apply or exclude a rule when a code is entered in the subject, and you wish this code to be removed from the subject. For instance, if you want to give users the possibility to disable a disclaimer for a particular message, you could have the user add a code to the subject of the email, for instance [Nodisclaimer]. You

can then create a rule in Policy Patrol that a disclaimer is added unless the subject contains the word [Nodisclaimer]. A further rule can be created to remove the code [Nodisclaimer] from the subject so that the recipient does not see the code in the subject.

- ❑ **Replace From: domain/email address:** Select this option if you wish to change the From: domain or email address. You might want to change this if you want to use a generic reply address such as [sales@domain.com](mailto:sales@domain.com), instead of the specific user's email address. To change the From: email address, enter the new email address in the top dialog. If you also want a display name to be shown, enter it as follows: "Display name" <user@domain.com>. To change the From: domain, enter the new domain in the bottom dialog (the original display name will be shown).

 **Note**

This option only works for externally sent messages.

- ❑ **Archive message:** Select this option to archive the message. In the options, select the archive to be used from the drop-down list. If you wish to create a new archive, click **New Archive**. Tick **Add billing code** to assign a billing code for the message in the archive. This can be useful if you wish to apportion email costs to internal departments or clients. Enter the billing code to be added to the archive.
- ❑ **Convert to plain text:** This option will convert the message to plain text. You might wish to do this to save bandwidth, or to remove any possible HTML embedded viruses. There are no further options for this action.
- ❑ **Change priority/importance:** With this option you can change the priority or importance of the message. Select 'High', 'Normal' or 'Low'.
- ❑ **Remove read receipt request:** If you select this option, Policy Patrol will remove the read receipt request.
- ❑ **Remove delivery receipt request:** If you select this option, Policy Patrol will remove the delivery receipt request.
- ❑ **Add From: domain/email address to filter:** This option will add the From: domain/email address to a predefined filter. This can for instance be useful to automatically build a list of spammers. It is quicker for Policy Patrol to block messages from certain email addresses or domains than it is to check for spam characteristics. Therefore, by

automatically adding the senders of spam messages to a spam email filter, next spam messages can be blocked more efficiently. Similarly, this option can be used to block senders of viruses. In the options, check the filter to add the From: domain or email address to. Select whether you wish the domain or the email address to be added to the filter. If you wish to create a new filter, click **New Filter**.

- ❑ **Add To: domain/email address to filter:** This option will add the To: domain/email address to a predefined filter. In the options, check the filter to add the To: domain or email address to. Select whether you wish the domain or the email address to be added to the filter. If you wish to create a new filter, click **New Filter**.

 **Note**

If the Administration console is open whilst a domain or email address is added to a filter, you must first close the console or disconnect (and not commit the changes) and then reopen it again, in order to see the new domains and/or email addresses in the filter.

- ❑ **Customize Delivery Status Notification:** With this option you can fully customize every Delivery Status Notification (DSN). In the options, select the notification(s) to be customized and the corresponding template(s). You can use the **All other notifications** option if you only wish certain notifications to use a custom template and all remaining notifications to use the same template. Note that by default the Delivery Status Notification will be sent in plain text. If you wish the Delivery Status Notification to be sent in HTML format, you must check the option **Use HTML format**. Policy Patrol will then use the text you entered in the HTML tab of the Template. There are some clients, such as UNIX clients that may not be able to read HTML mail. However, nowadays most clients can read HTML. If you wish Delivery Status Notifications to be sent in plain text only, leave the **Use HTML format** checkbox unchecked.

 **Note**

In the conditions of the rule you must specify whether the message should be a Success, Delay or Failure Delivery Status Notification. Only these notifications will be available for customization when configuring the action Customize Delivery Status Notification.

You can apply different templates to externally and internally sent DSNs by configuring two rules and applying one to externally sent messages and one to internally sent messages.

- ❑ **Add X-header:** This option can be used to add an X-header of a certain value to the mail. This can be of use if you wish an application to automatically process the mail or if you want to further process the message with an Outlook rule. In the options, enter the X-header to be added and the corresponding value. You can add multiple X-headers if you wish. Note that 'X-' is already added to the header, so you only need to enter 'Header' to have 'X-Header' added to the message.

#### Tip

If you wish an application to process certain emails, you can use Policy Patrol to select the messages to be processed on the basis of certain conditions and add an X-header to the mails. The application can then process all mails with this particular X-header. It is also possible to configure an Outlook rule that processes messages with the X-header. For instance, you can configure Outlook to place these messages in a separate folder in the user's inbox.

- ❑ **Add entry to log:** With this option you can add an entry to the Event Log and/or to the Policy Patrol Systems Events.
  - Add to Event Log:** Tick this option if you wish to add an entry to the Windows Event Log. Select the entry to be added by choosing a tag from the drop-down box. Select the event type, application name and Event ID to be added.
- ❑ **Add to Policy Patrol System Events:** Tick this option if you wish to add an entry in the tree node System Events in Policy Patrol. Select the entry to be added by choosing a tag from the drop-down box and selecting the event type.
- ❑ **Run application:** You can use this option to run an external program, for instance to send an SMS message or to beep a pager. Enter the path and file name or browse to the application to be executed by Policy Patrol. If you want to use any parameters, check **Parameters** and select the tag to be used. The tag can include fields such as the subject of the mail, or the name of the virus that was found. Tick **Wait for application to exit** if you want Policy Patrol to wait until the program has exited. By default Policy Patrol will wait up to 60 seconds for the program to exit. If the program has not exited by this time, Policy Patrol will end the process. If you want to change the time frame, you can do

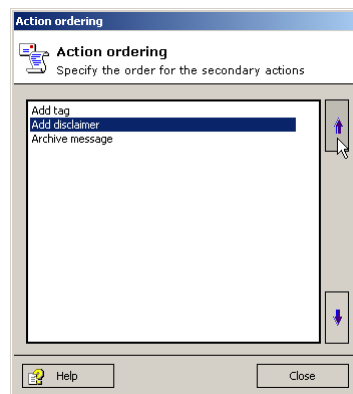
so by adding a System Parameter. Please send an email to [support@redearthsoftware.com](mailto:support@redearthsoftware.com) for more information on how to accomplish this.

 **Note**

If the application requires desktop interaction, you must tick the option ‘Allow service to interact with desktop’ in the Properties > Log On tab of the Policy Patrol Mail Processor service.

**Ordering of secondary actions**

By default Policy Patrol will apply the secondary actions in the order that they were selected. For instance, if you first select **Print message** and then **Add tag**, Policy Patrol will not include the tag in the printed message. If you wish to change the order of the secondary actions, you can do so by clicking on **Change order....** Then select the action and press the up or down arrow. The order you chose for the actions will be shown in the description window.

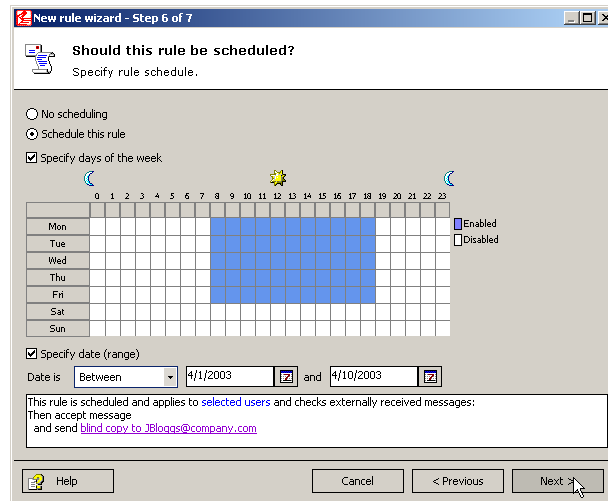


 **Note**

If you use fields such as subject, message body, attachment name in for instance a notification message, remember that if Policy Patrol is configured to add a tag, disclaimer or delete an attachment before sending a notification message, the fields will contain the altered values by Policy Patrol. If you wish the fields to include their original values, you must order the notification message on top.

**Step 6. Should this rule be scheduled?**

A rule can be scheduled to run for certain days or certain dates. If you do not wish to schedule the rule, click **Next**.



To specify the days the rule must run, tick **Specify days of the week**. Select the days and times the rule must run by clicking on the rows and columns or selecting individual boxes. The times and days that the rule is enabled will appear in blue.

To schedule the rule to run on certain dates, tick **Specify date (range)**. Specify the date by selecting **After**, **Before**, **Between** or **Not between** and entering the date(s). If you select **After** or **Before**, the rule will not run on the actual date selected, but after or before it. For instance, if you select that a rule must be triggered after January 1<sup>st</sup> 2003, it will be triggered on January 2<sup>nd</sup> 2003. If you select before January 1<sup>st</sup> 2003, the rule will be triggered on any date before, but not including January 1<sup>st</sup> 2003. If you select **Between** or **Not between**, the rule will be triggered or not be triggered between and including the dates selected. For example, if you configure a rule that should not be triggered between January 1<sup>st</sup> and January 3<sup>rd</sup> 2003, it will not be triggered on January 1<sup>st</sup>, January 2<sup>nd</sup> and January 3<sup>rd</sup> 2003.

 **Tip**

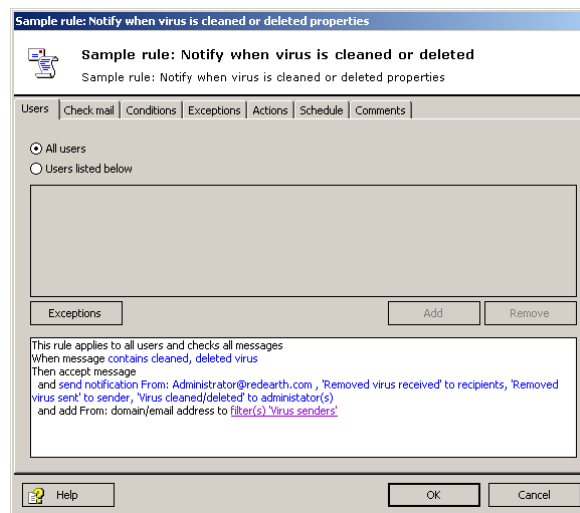
It can be useful to schedule a rule if for instance you wish to temporarily forward emails to someone else whilst the user is on holiday or on maternity leave.

**Step 7. Enter a name for the rule.**

In the final step, enter a name for the rule and any comments. Uncheck the **Enable this rule** box if you do not want the rule to be enabled right away. If you do not want any following rules to be processed, uncheck the option **Process following rule(s)**. At the bottom of the dialog, the estimated processing speed will be displayed. For more information on this, consult the paragraph 'Ordering rules'. Click **Finish** to create the rule.

## Editing existing rules

To edit an existing rule, go to Policy rules and select the rule to be edited. Then click on the **Properties** button. A dialog with seven tabs will appear. Make the changes in the appropriate tabs. Remember that you cannot change which messages to check without resetting all conditions and actions. If you want to change the name of a rule, right-click the rule in the list and select **Rename**.



### Note

Remember that after you make any changes in the Administration console, you must commit the changes by selecting server name > **Commit**, or by closing the Administration console and selecting 'Yes' when asked whether you wish to commit your changes. If you do not commit, the settings are not saved. The server name will be followed by a \* if there are any changes that have not yet been committed, i.e. server name\*.

## Ordering rules

In Policy Patrol you can order rules and select whether you wish to continue processing the following rules. The order of rules is important for efficiency reasons and for determining how messages should be processed.

### Processing speed

The way in which rules are ordered can be important for processing speed. For instance, it is quicker for Policy Patrol to check a list of domains or email addresses than it is to check for words in the body of an email. Therefore it

makes more sense to order fast rules above slow rules. Furthermore, if you have a rule that deletes viruses, it is better to order this rule to be first, since there is no use for an earlier rule to add a disclaimer to the message if it is deleted afterwards.

To help you order rules efficiently, Policy Patrol calculates the **estimated processing time** for each rule. This time can be fast, moderate or slow. Policy Patrol determines the speed of the rule by checking the following:

- ❑ Is the rule user-based? A user-based rule is slower to process than a global rule. If it is user-based, is it based on users or groups (groups are slower, especially large groups), and does it have user or group exceptions (user exceptions are faster than group exceptions)?
- ❑ Does the rule have conditions? In general, header conditions are fast to process. Searching for words in the message body or attachment is slower than searching for words in the subject or attachment name. However, the speed will also depend on the size of the filter. Policy Patrol looks at the condition and at the filter size and then calculates the estimated processing time.
- ❑ Which actions are chosen? Some secondary actions are more time intensive than others. Adding an X-header or changing message priority are fast, whereas adding disclaimers, tags or printing messages are more time consuming.

#### **Ordering result**

In addition to processing speed, it is also important to order the rules in such a way that the result is correct. For instance when adding multiple disclaimers, the order of the rules will determine the order in which the disclaimers are added to the message (see note below). Another example is a configuration with a rule that archives all mails and another rule that adds a disclaimer to outgoing mails. If your organization needs to prove that it added a disclaimer, you will need to place the disclaimer rule above the archive rule, since otherwise the archived messages will not include the disclaimer.

#### **Continue processing**

For each rule you can also specify whether Policy Patrol must continue to process the next rule. For instance, say you have a rule that quarantines confidential content and one that delays attachments larger than 5 MB. A message is received with confidential content and an attachment of 6 MB. The Administrator or Manager decides that the mail can be delivered and accepts the message. If you did not select **Process following rule(s)** in the quarantine rule, the message would be delivered regardless of the 6 MB attachment. If you selected to process the following rule, then Policy Patrol will consequently delay the message for delivery at the specified time. On the other hand, you might want to disable this option to avoid the message being quarantined multiple times. For instance, a message might be quarantined for offensive content. The manager views the mail and accepts it. If the mail now



gets quarantined again because it contains a picture, the manager would have to review the same mail again. To avoid this you can disable **Process following rule(s)**.

 **Note**

When ordering disclaimer and tag rules, the consecutive disclaimers or tags will be added as specified below. If you have two prepend disclaimer rules that apply to the same mail, the disclaimers will be applied as follows in the message:

Prepend Disclaimer 2

Prepend Disclaimer 1

If you have two append disclaimer rules, they will be applied as follows:

Append Disclaimer 1

Append Disclaimer 2

If you have two tag rules that are added to the subject, they will be added in the following order: Tag 2 Tag 1 Subject.

## Ordering conditions

There is no need to order conditions since if you have more than one condition or exception in a rule, Policy Patrol will automatically order the conditions so that processing is as fast as possible.

## Ordering secondary actions

By default Policy Patrol will apply the secondary actions in the order that they were selected. For instance, if you first select **Print message** and then **Add tag**, Policy Patrol will not include the tag in the printed message. If you wish to change the order of the secondary actions, you can do so by clicking on **Change Order...**

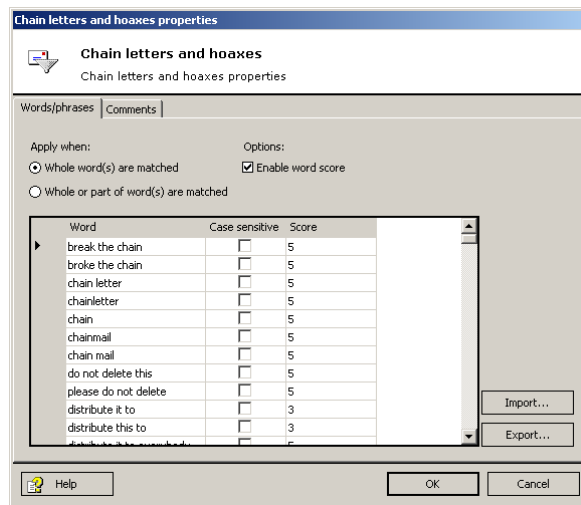
## Creating Filters

**F**ilters are lists of values that Policy Patrol must check. Policy Patrol includes Word/Phrase, Attachment Name, Attachment Type and Domain/Email Addresses filters. This chapter explains how to create each type of Policy Patrol filter.

### Creating a Word/Phrase filter

Word/Phrase filters contain lists of words and phrases that Policy Patrol must check for. The program includes a number of sample Word/Phrase filters. You can edit these sample filters, or create your own filter. To create your own Word/Phrase filter:

1. Go to **Filters** and click **New...**
2. When asked which type of filter you wish to create, select **Word/Phrase Filter**. Click **Next**.
3. Enter the word(s) or phrases to be included in the filter. For each word you can specify whether it should be case sensitive or not. If you check the **case sensitive** option, this means that Policy Patrol will only check for the word in the same case. This can be useful for certain spam or chain letters for instance, that tend to use a lot of capitals. For instance if a mail includes CLICK HERE in capitals there will be a good chance that the mail is spam. However, click here in lower case might be more innocent. By using the case sensitive option in conjunction with the **word score** option you could add both variations, applying a higher score to the upper case version. You can also apply a negative word score. For instance, this might be useful to eliminate some words that can be used innocently. For instance you might assign the word 'breast' a word score of 5, and assign the words 'baby' or 'chicken' a minus 5 score. When configuring the rule, you can specify the word score threshold that must be met to trigger the rule. If you do not wish to use word score in the filter, uncheck **Enable word score**.



Finally, select whether to apply when **Whole word(s) are matched** or when **Whole or part of word(s) are matched**. The first option allows you to specify more precisely which words must trigger a rule. For instance, if you select that **Whole or part of word(s) are matched** and you enter the word 'sex' in the filter, this will also include the words 'Sussex' and 'sextant'. If you select **Whole word(s) are matched**, the rule will trigger on the word 'sex' but not on 'Middlesex'.

#### Note

When checking for words/phrases remember that if word score is enabled, which it is by default, you must enter a word score threshold when configuring the rule. If you leave the threshold set to 0, the rule will trigger for every message.

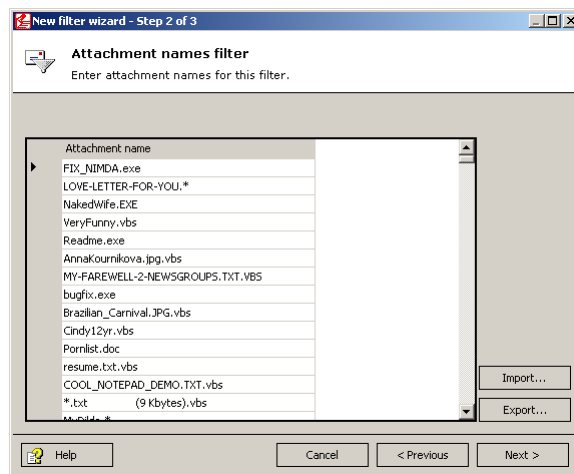
You can import lists from .txt files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. The format should be as follows: word/phrase,t/f,word score. Where t or f are true or false for case sensitive, and word score is the score you wish to assign for the word. For instance, if you wish to add the case sensitive word CLICK HERE with a word score of 5, you must enter it in the text file as follows: CLICK HERE,t,5. For every word or phrase you need to start a new line. If you import words or phrases from more than one file, the additional words or phrases will be added to the list. If you have two lists with some common words, Policy Patrol will not add the common words twice, but will only add the additional ones. To export the words in the filter, click **Export**, enter a file name and select **OK**. When you are ready adding words, click **Next**.

4. Enter a name for the filter and any additional comments. When you are done, click **Finish** to create the filter.

## Creating an Attachment Name filter

Attachment name filters include names of attachments that Policy Patrol must check for. Policy Patrol includes a number of sample attachment name filters. You can edit these sample filters, or create your own filter. To create a new Attachment Name filter:

1. Go to **Filters** and click **New....**
2. When asked which type of filter you wish to create, select **Attachment Name Filter**. Click **Next**.
3. Enter the attachment name(s). You can choose to enter an exact name, include an extension or only enter a word that must be found in a name. The more you enter the more exact the filter will be. For instance, if you enter `readme.exe`, the filter will only apply to the attachment `readme.exe`, not `readme.txt`. However if you enter `readme`, the filter will apply to the files `readme.exe` and `readme.txt`, and `readmetest.doc`. You can also use the wildcards `*` and `?`, where `*` stands for any amount of characters and `?` stands for one character. For instance, if you enter `licen?e`, it will find attachments named `license` and `licence` with any extension. Attachment names are not case sensitive. You can import lists from `.txt` files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. In the text file to import, each attachment name should be entered on a separate line. To export the attachment names in the filter, click **Export**, enter a file name and select **OK**. When you are ready adding file names, click **Next**.

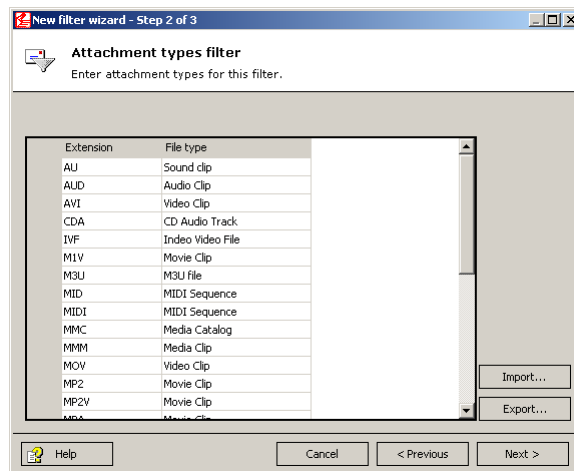


4. Enter a name for the filter and any additional comments. When you are done, click **Finish** to create the filter.

## Creating an Attachment Type filter

Attachment type filters contain lists of file extensions. Policy Patrol includes a number of sample attachment type filters. You can edit these sample filters, or create your own filter. To create your own attachment type filter:

1. Go to **Filters** and click **New...**
2. When asked which type of filter you wish to create, select **Attachment Type Filter**. Click **Next**.
3. Enter the extension and optionally enter the file type. For example, enter `zip` as the extension and enter `archive` as the file type. Do not enter the full stop in front of the extension. You can import lists from `.txt` files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. You must enter the file extensions as follows: `file extension,file type`. Enter each attachment type on a separate line. To export the attachment types in the filter, click **Export**, enter a file name and select **OK**. When you are ready adding file names, click **Next**.



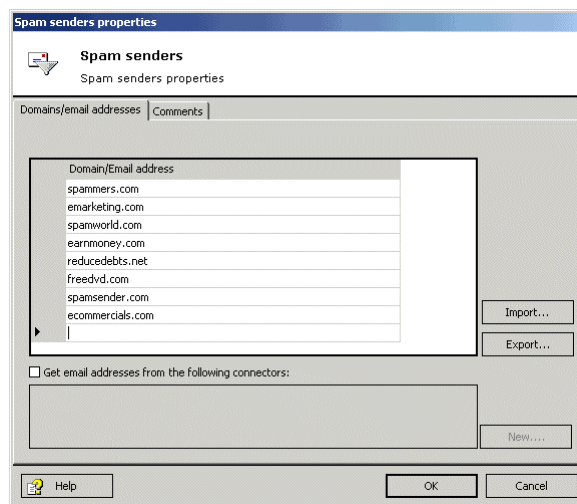
4. Enter a name for the filter and any additional comments. When you are done, click **Finish** to create the filter.

## Creating a Domain/Email Address filter

Domain/Email address filters contain lists of domains and email addresses to filter on. Policy Patrol includes a number of sample Domain/Email address filters. You can edit these sample filters, or create your own filter. To create a new Domain/Email address filter:

1. Go to **Filters** and click **New...**

- When asked which type of filter you wish to create, select **Domain/Email Address Filter**. Click **Next**.
- Enter the email addresses and domains in the list. 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. If you wish to add addresses from the Active Directory or your mail server, you can select the option **Get email addresses from the following connectors**. For instance, in this way you can use a list of Active Directory contacts. These lists will then be continually updated every time Policy Patrol synchronizes with the Active Directory. Check the connectors you wish to use. If you wish to create a new connector for the filter, click **New**. You can import lists from .txt files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. In the text file to import, each domain/email address should be entered on a separate line. To export the filter, click **Export**, enter a file name and select **OK**. When you are ready, click **Next**.



- Enter a name for the filter and any additional comments. When you are done, click **Finish** to create the filter.

## Editing filters

To edit an existing filter, select the filter and click **Properties**. A tabbed dialog will now appear. You will be able to add or delete entries and change the comments for the filter. If you edit a filter that is already being used in a rule, the filter will automatically be updated for the rule. You can change the filter name by right-clicking on the filter in the list and selecting **Rename**.

 **Note**

If you rename a filter that has already been configured for a rule, the rule will continue to work for the filter, but the filter name in the description will still be the old name. To update the filter name, you need to open the rule properties and open the dialog where the filter is selected. Click **OK** to save the new name in the rule.

## Creating Templates

**T**emplates are pre-configured texts that can be used in Policy Patrol rules. The program includes three types of templates: Notifications, Tags and Disclaimers. This chapter explains how to create each type of Policy Patrol template.

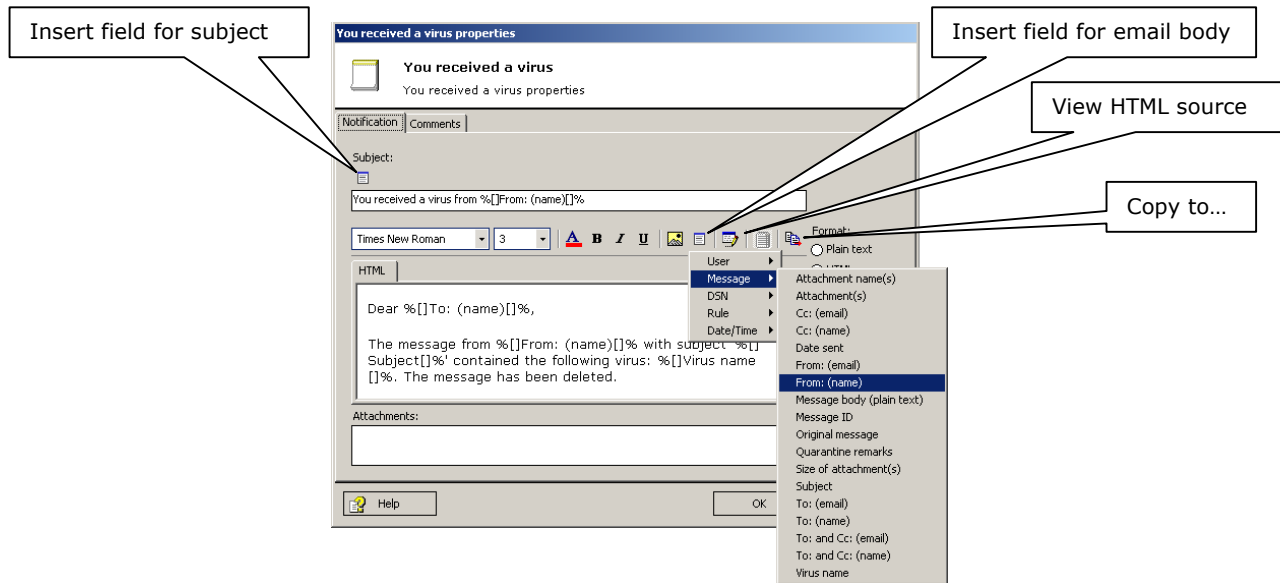
### Creating a Notification template

Notification templates are used for notification messages, approve/reject notifications and Delivery Status Notifications. Policy Patrol includes a number of sample notification templates. You can edit these sample templates or create your own. To create a new Notification template:

1. Go to **Templates** and click **New....**
2. When asked which type of template you wish to create, select **Notification Template**. Click **Next**.
3. Enter the subject for the notification email. You can include fields in the subject by clicking on the **Insert Field** button above the subject line. For more information on available fields, see the 'Fields' paragraph.

The notification message body can be in plain text, HTML or both. Select both if you are not sure whether the recipient can read HTML messages. Although nowadays most clients can read HTML, there are still some older clients that can only read plain text emails. If you select both, make sure that text is entered in both tabs. To copy text from one tab to the other, click on the **Copy to..** button on the far right of the toolbar. When you select the Plain text tab, all formatting options will be disabled. You can insert fields in the body of the message by clicking on the **Insert Field** icon in the toolbar and selecting the relevant field.





The text can be formatted by selecting font type, size or color and applying bold, italicized or underlined styles. You can insert gif and jpeg pictures by clicking on the **Insert image** button. Browse to the picture and click **Select**. If you wish to add HTML tags, for instance to add tables or bullets, you can edit the HTML source by clicking on the **View HTML source** button. To add an attachment to the notification, click on **Add....** Select the attachment and click **Select**.

 **Note**

If you use user fields in notification messages, the fields are taken from the sender of the message that triggered the rule.

If you want to include a link to a quarantined message, click on the **View HTML source** button and enter `<A href="http://IP address/PolicyPatrolWebMonitor/main.aspx?ID=%[]Message code[]%">Enter your link text here</A>`, for instance `<A href="http://100.0.0.1/PolicyPatrolWebMonitor/main.aspx?ID=%[]Message code[]%">View inappropriate email</A>`.

You can import texts from .txt and .html documents by clicking **Import**. Similarly, you can export the text to a .txt or .html file by clicking **Export**. When you are ready, click **Next**.

4. Enter the template name and possible comments. Click **Finish** to create the template.

 **Tip**

If you are not sure whether a field will exist in every instance, you can specify a **field prefix** that will only be entered if the field is replaced. For instance, if you wish to include a mobile phone number for the user, but not every user has one, you could enter the prefix in between the first square brackets of the field as follows: %[Prefix]Field name[]%. For instance: %[Mobile:]Mobile phone[]%. This will mean that the text 'Mobile:' will only be added if the user has a mobile phone number in the user's Active Directory, Exchange 5.5 or Lotus Domino properties.

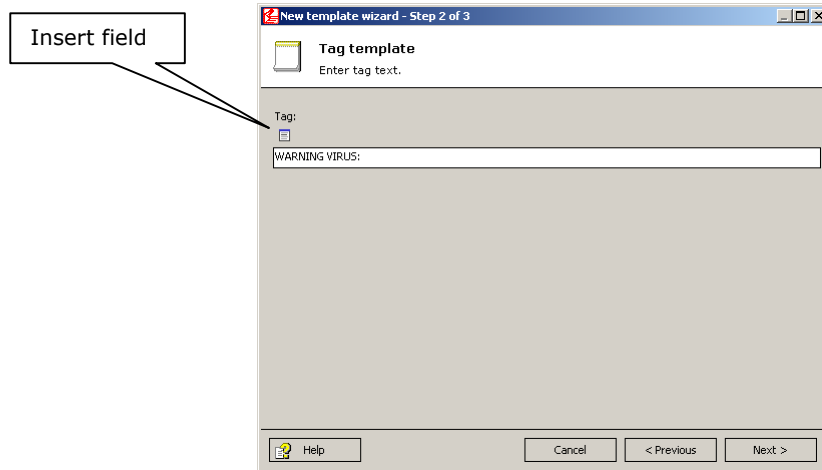
It is also possible to specify a **default value** in case a field does not exist. For instance, if a user does not have a mobile phone number, you could enter 'Not applicable'. To do this, you must enter the default value in between the last square brackets of the field as follows: %[]Field name[Default value]%. For example: %[]Mobile phone[Not applicable]%.

Note that you cannot enter fields as a prefix or default value.

## Creating a Tag template

Tags can be placed in front of an email subject or in an archive. Furthermore, they are used for network messages, log entries, application parameters and compression comments. Policy Patrol includes a number of sample tags. You can edit these sample templates or create your own. To create your own Tag template:

1. Go to **Templates** and click **New....**
2. When asked which type of template you wish to create, select **Tag Template**. Click **Next**.
3. Enter the text for the tag. You can also use fields by clicking on the **Insert field** button. For more information on the available fields, see the 'Fields' paragraph. Click **Next**.



4. Enter the template name and possible comments. Click **Finish** to create the template.

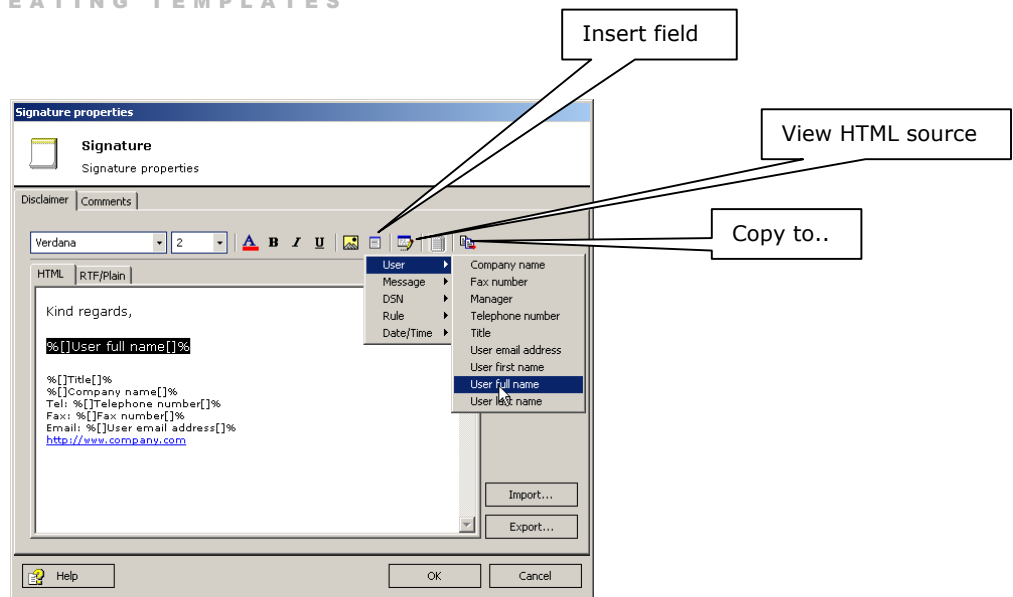
## Creating a Disclaimer template

Disclaimer templates are used for adding disclaimers and signatures to messages. Policy Patrol includes a number of sample disclaimer templates. You can edit these sample templates or create your own. To create your own Disclaimer template:

1. Go to **Templates** and click **New....**
2. When asked which type of template you wish to create, select **Disclaimer Template**.

Enter the text for the disclaimer. You can enter the text in two different formats: HTML and RTF/plain text. The text in the HTML tab will be added to HTML messages, and the text in the RTF/plain text tab will be added to rich text and plain text messages. If you don't enter any text in the HTML tab, there will be no disclaimer added to HTML messages. If you don't enter any text in the RTF/plain text tab, there will be no disclaimer added to rich and plain text emails. Because some email clients can only read plain text, you must always enter a disclaimer text in the RTF/plain text tab, even if you only send out HTML messages. However, you only need to enter your text once, since you can copy and paste the text from one tab to another by clicking on the **Copy to..** button on the far right of the toolbar.

You can apply formatting in the RTF/plain text tab, but this will only apply to rich text messages. The formatting will be removed for plain text messages. In the HTML tab you can add HTML tags, for instance to add tables or bullets. To do so, you can edit the HTML source by clicking on the **View HTML source** button.



You can insert fields by clicking on the **Insert Field** icon and selecting the relevant field. For more information on the available fields, see the 'Fields' paragraph. You can import texts from .txt and .html documents by clicking **Import**. Similarly, you can export the text to a .txt or .html file by clicking **Export**. If you wish to add a picture, click on the **Insert image** icon, browse to the picture and click **Select**. Remember that if you are configuring Policy Patrol remotely, you will be able to select from pictures on the local drive of the server installation, but you will not be able to view the pictures remotely. When you are ready, click **Next**.

### Tip

If you are not sure whether a field will exist in every instance, you can specify a **field prefix** that will only be entered if the field is replaced. For instance, if you wish to include a mobile phone number for the user, but not every user has one, you could enter the prefix in between the first square brackets of the field as follows: %[Prefix]Field name[]. For instance: %[Mobile:]Mobile phone[]. This will mean that the text 'Mobile:' will only be added if the user has a mobile phone number in the user's Active Directory, Exchange 5.5 or Lotus Domino properties.

It is also possible to specify a **default value** in case a field does not exist. For instance, if a user does not have a mobile phone number, you could enter 'Not applicable'. To do this, you must enter the default value in between the last square brackets of the field as follows: %[Field name][Default value]%. For example: %[Mobile phone][Not applicable]%

Note that you cannot enter fields as a prefix or default value.

3. Enter the template name and possible comments. Click **Finish** to create the template.

 **Note**

Usually, HTML and rich text messages include a plain text version of the email, which is displayed if the email client cannot read HTML or rich text formatted mails. Therefore you must always enter the disclaimer text in plain text format since if you only entered the disclaimer text in HTML format, this would cause the email clients not capable of displaying HTML formatted messages, not to see the disclaimer.

## Editing templates

To edit an existing template, select the template and click **Properties**. A tabbed dialog will now appear. You will be able to add or delete entries to the filters and change the comments for the template. To rename a template, right-click on the name in the list and select **Rename**.

 **Note**

If you rename a template that has already been configured for a rule, the rule will continue to work for the template, but the template name in the description will still be the old name. To update the template name, you need to open the rule properties and open the dialog where the template is selected. Click **OK** to save the new name in the rule.

## Fields

Policy Patrol includes user fields, message fields, DSN fields, rule fields and date/time fields. Each type of field is described below.

### User fields

The user fields are taken from Active Directory, Exchange 5.5 or Lotus Domino, depending on the type of connector the user is retrieved from. Below is a list of the user fields that are included by default. Some of these fields are only applicable if you have Active Directory (see note below). You can add more (or remove) fields by going to Server name > **Properties** > **User fields** tab. More information on how to do this can be found in the 'Advanced options' chapter.

Default field	Description
Company name	Company's name
Fax number	User's fax number
Manager	User's manager (only for Active Directory)
Telephone number	User's telephone number
Title	User's title
User email address	User's email address
User first name	User's first name
User full name	User's full name
User last name	User's last name

The following fields can be enabled by placing a check in front of the field name in Server name > **Properties** > **User fields** tab:

Default field	Description
Company street	Company's street address (only for Active Directory)
Company P.O. Box	Company P.O. Box (only for Active Directory)
Company city	Company's city
Company state	Company's state
Company zip code	Company's zip code
Company country	Company's country
Mobile phone	User's mobile phone

#### Note

Some of the default user fields are only applicable if you have Active Directory. If you have **Exchange 5.5** most fields are the same, apart from 'Manager', 'Company street' and 'Company P.O. Box'. To use the company address, you must create a new field in Server name > Properties > User fields, using the code 'postalAddress' for the company address. If you have **Lotus Domino**, most fields are the same apart from 'Manager', 'Company name', 'Company street', 'Company P.O. Box' and 'Company country'. To use these fields you will need to create Lotus Domino specific user fields. For more information about how to add new user fields, see the 'Advanced options' chapter.

#### Message fields

In addition to user fields, Policy Patrol includes merge fields that are related to the email message, such as subject and date sent. Below is a list of available message fields.

Field	Description
Attachment name(s)	Name(s) of the attachments.
Attachment(s)	The attached file(s).

Cc: (email)	Email address in the Cc: field.
Cc: (name)	Name in the Cc: field (If the name is not known, the field will be replaced by the email address in the Cc: field).
Date sent	Date the message was sent.
From: (email)	Email address in the From: field.
From: (name)	Name in the From: field.
Message body	The message text. This will always be in plain text.
Message ID	The unique ID of the message.
Original message	The original message including attachments. The message can only be opened if it was an external message. See the note below.
Quarantine remarks	This field will be replaced with any remarks that are entered when accepting or rejecting the message.
Size of attachment(s)	Size of the attachment(s). If there are multiple attachments this field will state the combined size.
Subject	Subject of the message.
To: (email)	Email address in the To: field.
To: (name)	Name in the To: field (If the name is not known, the field will be replaced by the email address in the To: field).
To: and Cc: (email)	Email address(es) in the To: and Cc: fields.
To: and Cc: (name)	Name(s) in the To: and Cc: fields (If the name is not known, the field will be replaced by the email address in the To: or Cc: field).
Virus name	The name of the virus as identified by the anti-virus engine.

 **Note**

The **Original message** field only works for external mails. If a notification includes this field and the original message was internal, the message is attached but will be empty. The reason for this is that the internal message will be in a proprietary format of Exchange server.

**DSN fields**

These fields can only be used for Delivery Status Notifications and offer the possibility to customize DSN notifications. The following DSN fields are available:

Field	Description
Action	Success, Delay or Failure.

Arrival Date	Date the email arrived, e.g. Fri, 27 Sep 2002 13:46:16 +0300.
Body	The text of the DSN message.
Diagnostic Code	Explanation of the DSN.
Final Log ID	Final Log ID.
Final recipient	Final recipient of the message, which can be different from the original recipient.
Gateway	Gateway of the message.
Last attempted	Last attempted delivery.
Original recipient	Original recipient of the message.
Received MTA	The MTA from which the reporting MTA received the message.
Remote MTA	A remote MTA is an MTA that cannot or refuses to deliver the message.
Retry until	Retry delivery until.
Status	The number of the DSN report, for instance 5.7.1 for a failure notification.
Reporting MTA	The MTA that reports the results of the delivery attempt.

 **Note**

When you are creating DSN notification templates, remember that any message fields you insert will relate the notification itself, not to the originally sent message. Therefore, to enter the recipient email address of the original message, you must use the DSN fields **Original recipient** and **Final recipient**.

**Rule fields**

These fields relate to the rule that the message triggered. The following fields are available:

Field	Description
Rule name	Name of the rule that triggered.

**Date/Time fields**

These fields relate to the date and time the message was sent. Below is a list of available fields.

Field	Description
Date (numerical)	For instance, 08/28/2002
Day (numerical)	For instance, 28
Day of the week	For instance, Wednesday
Month (numerical)	For instance, 08



## CREATING TEMPLATES

Date and time	For instance, 08/28/2002 14:05
Time	For instance, 14:05
Year	For instance, 2002

## Monitoring messages

This chapter discusses the different ways in which you can monitor quarantined, delayed and deleted messages and how to approve or reject messages on hold.

### Monitoring messages from Policy Patrol

Messages can be monitored from the Policy Patrol Administration console > **Monitoring**.

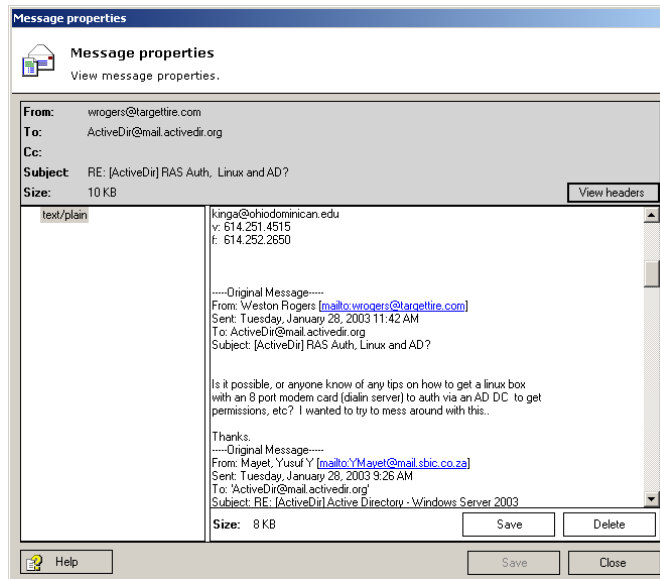
#### **Last 50 messages processed by Policy Patrol**

This dialog includes an overview of the last 50 emails processed by Policy Patrol. The list is continually updated and displays the time, sender, recipient and subject of the message, as well as the rule(s) triggered, if any.

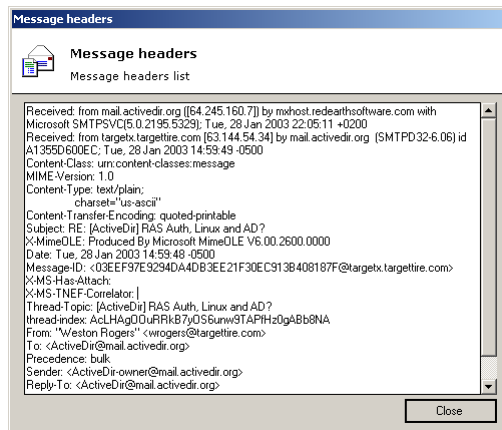
#### **Viewing quarantined, delayed and deleted messages**

To view messages on hold, click on the **On hold** button. You will now see a list of all quarantined and delayed items. To view only quarantined mails, click on **Quarantine**. To view only delayed mails, click on **Delayed**. To view Deleted messages, click on the **Deleted** button. By default all messages will be displayed. If you only wish to see messages caught by a certain rule, you can select the appropriate rule from the drop-down box in the top right corner.

The Quarantined, Delayed and Deleted lists will display the From, To: and Cc: field, Subject and Attachment name(s) of the message, rule that was triggered and the date and time it was sent. To refresh the list, activate another tree node and click on the respective tree node again. To view the properties of the message, double-click on the message or select the message and click **Properties**.



In the Message properties you will be able to view From:, To:, Cc: , Subject, message size, message headers, message body text, and attachment size. The total message size is displayed in **Size** box at the top left of the dialog. To view the message headers, click on **View headers....**



To view the message text, click on the message body in the left pane. For external messages, the message body will be displayed as **text/plain** and/or **text/html**. For internal messages, the message body will be displayed as **Message body**. When selected, the message text will be displayed in the right pane. For HTML messages the HTML source will be shown. This is a safety precaution so that any potential scripts will not run.

 **Note**

The figure in the message size dialog will not be exactly the same as the sum of the separate message parts, since there are other parts of the message such as headers that are also counted in the total message size. Furthermore, the message parts can be encoded differently, which also causes their size to differ.

**Saving down and deleting attachments**

To check whether an attachment is safe, you can save down the selected attachment by clicking **Save**. To delete an attachment, select the attachment and choose **Delete**. To view the attachment size, select the attachment. The size will be displayed after **Size:** at the bottom of the dialog.

For internal mails attachments are displayed as follows: **attachment [attachmentname.extension]**. For instance for a pdf attachment: attachment [brochure.pdf]. For external messages they are displayed as follows: **attachment type description [attachmentname.extension]**. For instance for a zip attachment: application/x-zip-compressed [archive.zip].

Attached messages will appear as follows for external mails: **message/rfc822**. For internal mails, the embedded message will appear as **attachment [Untitled Attachment]**. For external messages you will be able to view the content of embedded messages. This is not possible for internal mails.

**Removing body parts**

Sometimes you can remove body parts of a message. For instance, for HTML messages there is usually an HTML and plain text part to the message. If you do not wish the user to receive the HTML version of the mail (because it includes a potentially harmful script for instance), but still wish the user to receive the plain text version, you can delete the HTML part. If there is more than one body part to a message, it will say **multipart/alternative**. There will be a **text/plain** part and a **text/html** part. You can delete one of these body parts if you wish. By deleting the html part you will disable any potential scripts or viruses. By deleting the text part you will reduce the size of the message (slightly).

 **Note**

Internal messages always have only one body part. Therefore you cannot delete this body part since this would effectively mean deleting the whole message. If you want to delete the entire message, you must select the message and choose **Reject**.

**Tip**

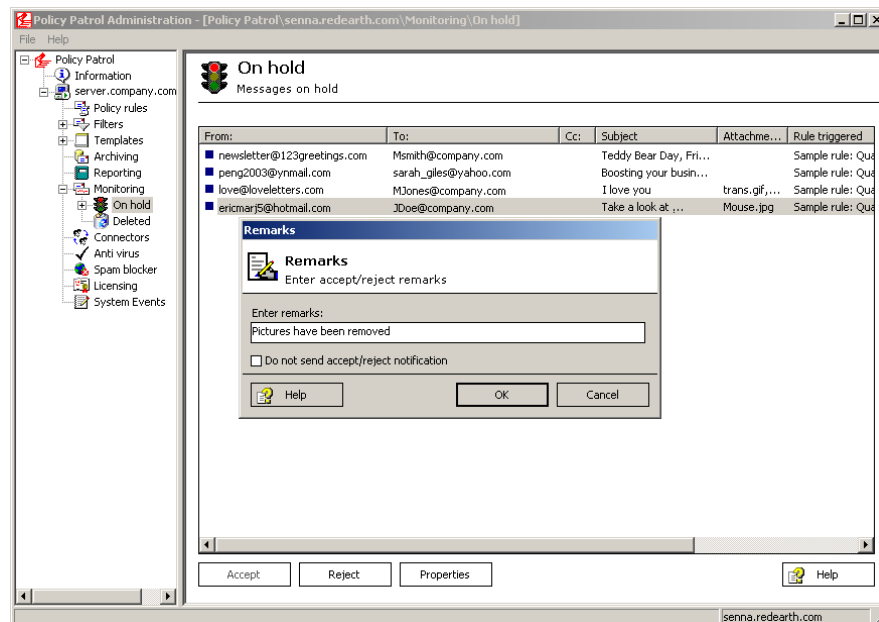
For more information on the naming conventions used in the Message properties dialog, please consult RFC 822 at the following url: <http://www.faqs.org/rfcs/rfc822.html>.

**Adding senders and recipients to filters**

You can add senders and recipients of quarantined messages to filters by selecting the relevant message(s), right-clicking, and selecting **Add sender to filter** or **Add recipient(s) to filter**. Then select the filter the sender or recipient should be added to. This option can be useful if you have false positives and wish to add the sender or recipient to a white list, such as the sample Newsletter filter.

**Accepting messages on hold**

To accept a quarantined mail or deliver a delayed mail, select the message and click **Accept**. If you selected a quarantined message, a dialog will pop up asking you to enter any remarks. If you wish to add a comment, enter it here and click **OK**. The comments will be entered in the **Quarantine remarks** field in the Accept notification template. This can be useful if you wish to inform the recipient that you have removed an attachment, or that you have converted the message to plain text (i.e. deleted the HTML body part). As soon as you click **Accept**, the accept notification(s), if configured, will be sent. If you do not want an accept notification to be sent for the selected message(s), tick the option **Do not send accept/reject notification**. To accept multiple messages, select the appropriate messages and click **Accept**. If you enter a remark, the remark will be added for each of the selected messages notification(s).



**Rejecting messages on hold**

To delete the quarantined or delayed message, select **Reject**. If you selected a quarantined message, a dialog will pop up asking you to enter any remarks. If you wish to add a comment, enter it here and click **OK**. The comments will be entered in the **Quarantine remarks** field in the Reject notification template. As soon as you click **Reject**, the reject notification(s), if configured, will be sent. If you do not want an accept notification to be sent for the selected message(s), tick the option **Do not send accept/reject notification**. To reject multiple messages, select the appropriate messages and click **Reject**. If you enter a remark, the remark will be added for each of the selected messages notification(s).

**Undeleting deleted messages**

Policy Patrol stores deleted messages in the deleted folder. If you wish to restore an email go to **Monitoring > Deleted**, select the message and choose **Undelete**. Policy Patrol will now deliver the message.

## Monitoring messages via the web

With the Policy Patrol web monitor you can view, accept and reject messages on hold from anywhere, just as long as you have an Internet or intranet connection. To use the web monitor:

1. Open Internet Explorer.
2. Enter the IP address of the Policy Patrol machine, followed by /PolicyPatrolWebMonitor. For instance:  
<http://10.3.0.25/PolicyPatrolWebMonitor>.
3. You will now be able to view all quarantined, delayed and deleted messages. To view the properties of the message, click on the link in the From: field.
4. To accept a message, select the message and click **Accept**. To reject a message, select the message and click **Reject**. If you wish to add some remarks you can enter these in the Remarks dialog box. The remarks will be entered in the 'Quarantine remarks' field of the accept or reject notification template. If you select more than one message you can accept or reject these in one go. If you enter a remark, the remark will be added for each of the selected messages notification(s).

## Monitoring messages via email

When you create a rule and specify that the mail must be quarantined, delayed or deleted, you can configure a notification message that is sent to an Administrator, Manager or other recipient for approval/rejection. This message can include a direct link to the quarantined/delayed/deleted email in question.

## MONITORING MESSAGES

The link will open up the web monitor and show the particular message. From here the administrator or manager can view the mail and accept, reject or undelete it. By clicking on **Quarantined items**, a list of all messages will appear.

You can add a link to a quarantined, delayed or deleted message by entering the IP address of the Policy Patrol machine followed by:

`/PolicyPatrolWebMonitor/main.aspx?ID=%[]Message code[]%`, for instance:  
`http://100.0.0.1/PolicyPatrolWebMonitor/main.aspx?ID=%[]Message code[]%`.

To include a link in a notification message, click on the **View HTML source** button and enter `<A href="http://IP address/PolicyPatrolWebMonitor/main.aspx?ID=%[]Message code[]%">Enter your link text here</A>`, for instance `<A href="http://100.0.0.1/PolicyPatrolWebMonitor/main.aspx?ID= %[]Message code[]%">View inappropriate email</A>`.

## Archiving

**M**essages and their attachments can be archived by Policy Patrol. This chapter discusses the different archiving options that can be configured.

### SQL archiving

If you wish to use SQL archiving and SQL server is not installed on the Policy Patrol machine, you must install Microsoft Data Access Components (MDAC) 2.6 or later. This is because Policy Patrol uses MDAC for connecting to the SQL database. You can download MDAC from:

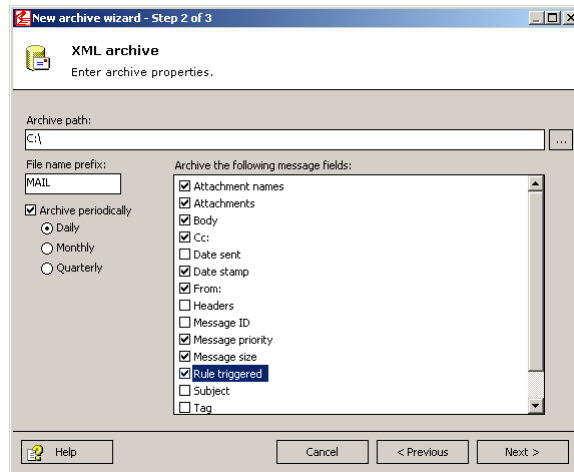
[http://www.microsoft.com/data/download\\_26sp2.htm](http://www.microsoft.com/data/download_26sp2.htm).

### Creating an archive

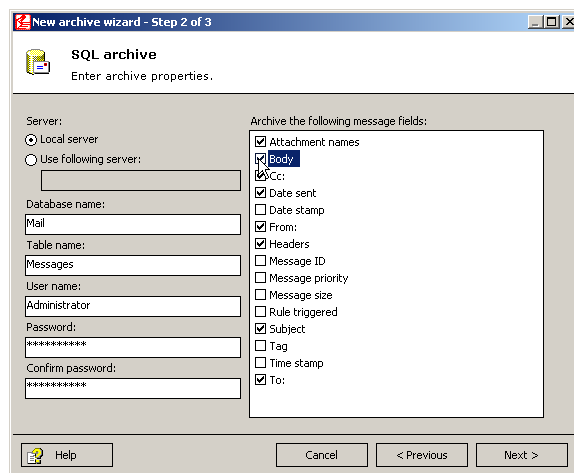
Policy Patrol includes the possibility to archive messages and their attachments in XML, CSV or SQL archives. Policy Patrol includes a sample archive. You can edit this archive or create your own. Follow the next steps to create an archive:

1. Go to **Archive** and click **New...**
2. In the Archive Type dialog, select **XML archive**, **CSV archive**, or **SQL archive**.
3. Configure the archive properties.





**For XML and CSV archives:** In **Archive path**, enter the path to the drive or folder for storing the archive. Alternatively click ... and browse to the folder. In **File name prefix**, enter the prefix that should be added to the archive file, for instance MailArchive. Select whether you wish to **archive periodically**. You can create a new archive daily, monthly or quarterly. If you select daily, the following suffix will be added to the file name: Dyyyyymmdd, e.g. MailArchiveD20020926. If you select monthly the following suffix will be added: Myyyyymm, e.g. MailArchiveM200209. The following suffix will be added if you select Quarterly: Qyyyyyq, where q stands for the quarter in question. For instance MailArchiveQ20023 is the archive for the 3<sup>rd</sup> quarter of 2002. If you do not enable archive periodically, the complete archive will be kept in one file. In this case, the file will include the suffix U, e.g. MailArchiveU.



**For SQL archives:** Select the SQL server machine. If it is on the same machine as Policy Patrol, select **Local server**. If it is installed on a different server, select **Use following server** and enter the name or IP address of the machine. Enter the database name and table name for storing the

messages. Specify the user name and password of an account with access rights to the SQL server.

Now select the message fields to archive. You can select the following fields:

Message field	Description
Attachment names	Names of attachment(s).
Attachments*	Attached file(s). A link will be included to the saved file, which will be located in the 'attachments' subfolder.
Body	Body text of the message.
Cc:	Cc: email address(es).
Date sent	Date and time, e.g. 09/26/2002 11:59:29.
Date stamp	Date, e.g. 09/26/2002.
From:	From: email address.
Headers	Headers of the message.
Message ID	The unique ID of the message.
Message priority	High, Low or Normal.
Message size	Total size of the message including attachment(s).
Rule triggered	The name of the rule that triggered.
Subject	Subject.
Tag	Tag (you must select to add tag to archive in a rule).
Time stamp	Time, e.g. 11:59.
To:	To: email address(es).

\* Only available for XML and CSV archives.

When you are ready, click **Next**.

4. Enter the Archive name and any comments you wish to add. Click **Finish** to create the archive.

## How to archive messages

You can specify which messages should be archived by creating a policy rule. If you wish all messages to be archived, follow the next steps to create the rule:

1. Go to **Policy rules** and click **New...**
2. In the Users dialog, select that the rule should apply to **All users**. Click **Next**.

3. Check **Sent** and **Received** for Internal messages and **Sent** and **Received** for External messages. Click **Next**.
4. Leave **No conditions** enabled. Click **Next**.
5. Leave **No exceptions** enabled. Click **Next**.
6. Select **Accept message** as the primary action. Tick **Archive message** as the secondary option. Click on the **archive** link and select the archive from the list. You can also create a new archive from here by clicking on **New Archive...** Optionally you can add a billing code, although this feature is more useful when you have selected specific messages to be archived since otherwise all messages will simply have the same billing code added. Click **Next**.
7. Leave **No scheduling enabled**. Click **Next**.
8. Enter 'Global archive rule' as the name, leave **Enable this rule** and **Process following rule(s)** checked and enter the following comments: 'This rule archives all messages to [archive name]'. Click **Finish** to create the rule.

## Viewing archived attachments

If you select to archive the message field **Attachments**, the attached files will be stored in the 'attachments' subfolder. The XML or CSV file will include the full path to the file, so that you will be able to click on the link to view the attachment.

### **Note**

If the same attachment is sent multiple times, the additional attachments will have a number added after the file extension. For instance if you email Document.doc and then resend the same document, the second file will be called Document.doc.1, the third will be Document.doc.2, etc. To open these files, you must first delete the numerical extension.

## Reporting & logging

**P**olicy Patrol can create reports on all mails that have been logged. This chapter discusses the different logging and reporting options in Policy Patrol.

### Logging

Policy Patrol offers two different types of logging:

1. **Message flow logging:** this type of logging records the details of all emails that pass through Policy Patrol. Details that can be logged include: date sent, from, to, cc, bcc (only if sent), subject, attachment name and message size. These logs can be used for creating reports. The settings for message flow logging can be configured in Computer name > **Properties** > **Message flow logging** tab. For more information, consult the 'Advanced options' chapter.
2. **System logging:** this type of logging records any errors that Policy Patrol may report. The settings for system logging can be configured in Computer name > **Properties** > **System logging** tab. For more information, consult the 'Advanced options' chapter.

#### **Note**

If you wish to keep a copy of sent and or received attachments you can do this by creating an archiving rule.

### Creating a report template

To generate reports, you must first create a report template where you specify what should be included in the report. You can then run this report as many

times you wish, specifying in each instance which reporting period should be used. To create a report template:

1. Go to **Reporting** and click **New**. The Report wizard will appear.
2. In **Report type**, select the type of report template you wish to create. Policy Patrol includes the following report types:

Report template	Description
Traffic by local domain	Number of messages and their size per local domain.
Traffic by local users	Number of messages and their size per local user, grouped by local domain.
Traffic by local domain to and from external domains	Number of messages and their size per local domain to and from certain external domains.
Traffic by local users to and from external domains	Number of messages and their size per local user to and from certain external domains.
Traffic by local users to and from other local users	Number of messages and their size between local users.
Attachments by local domain	Number of attachments per local domain.
Attachments by local users	Number of attachments per local user.
Attachments by local domain to and from external domains	Number of attachments per local domain to and from certain external domains.
Attachments by local users to and from external domains	Number of attachments per local user to and from certain external domains.
Attachments by local users to and from other local users	Number of attachments between local users.
Attachment types by local domain	Attachment types per local domain.
Attachment types by local users	Attachment types per local user.
Attachment types by local domain to and from external domains	Attachment types per local user main to and from certain external domains.
Attachment types by local users to and from external domains	Attachment types per local user main to and from certain external domains.
Attachment types by local users to and from other local users	Attachment types between local users.

Rules triggered by local domain	Rules triggered per local domain.
Rules triggered by local users	Rules triggered per local user.
Rules triggered by external domains	Rules triggered per external domain.

Layout options can be specified in the report header and report footer columns. To include a header and/or footer, select the option **Include the following fields** in the respective column. Tick the fields that you wish to include in the header or footer. Click **Next**.

3. Select the report conditions. If there are no conditions, click **Next**. If you only wish to include certain messages in the report, select **Use report conditions** and select the conditions that should be matched. For instance, you might want to generate a report of the messages that were sent and received by the Accounts department. You would then select **Traffic by local users** as the report type, and then select the conditions From:, To: and Cc: is member of Accounts Group.

If any of the conditions must be met, select **Match any of the conditions**. For instance, if you want to generate a report of the messages that were sent or received by the Accounts department, you must select the Accounts department in From: is member of group and To: is member of group, and select match any condition. If all the conditions must be met, select **Match all of the conditions**. For instance, if you wish to create a report on all messages sent by the Accounts department at a particular time, you need to select match all conditions.

Below is a list of available conditions. When you are ready, click **Next**.

### General

- Message is of date:** Select this option to only include messages of a certain date. Click on the **date** link and specify whether the message date must be equal, after, before, between or not between certain dates. If you select **before** or **after**, the date itself will not be included. For instance, if you specify that a rule should trigger for dates before October 1<sup>st</sup>, the rule will trigger for messages sent on or before September 30<sup>th</sup>, but not on October 1<sup>st</sup>. If you select **between** or **not between**, this will include the two values. For instance, if you select **between** 5<sup>th</sup> and 7<sup>th</sup> September, the rule will trigger for messages sent on 5<sup>th</sup>, 6<sup>th</sup> and 7<sup>th</sup> September. If you select **not between** 5<sup>th</sup> and 7<sup>th</sup> September, the rule will not trigger for messages sent on 5<sup>th</sup>, 6<sup>th</sup> and 7<sup>th</sup> September.

 **Note**

Remember that when you run the report later you will specify the reporting period by selecting the log file to be used for generating the report. You can use this date option if you for instance have monthly logging enabled but wish to generate a report for particular days or weeks.

- Message is of time:** Select this option to only include messages of a certain time. Click on the **time** link and specify whether the message date must be before, after, between or not between certain times. If you select **before** or **after**, the time itself will not be included. If you select **between** or **not between**, this will include the two times.
- Message is of size:** Select this option to only include messages of a certain size. Click on the **size** link and specify whether the message size (this includes headers, message text and attachments) should be greater than, less than, between or not between certain values. If you select **Greater than** or **Less than**, the value you enter will not be included, e.g. if you select greater than 1 MB, the rule will trigger on a message of 1.1 MB, but not on 1 MB. If you choose **Between** or **Not between**, the values you enter will be inclusive, e.g. if you specify that the message size should be between 2 and 3 MB, the rule will trigger for messages of 2 MB and 3 MB and any size in between. If you select not between 2 and 3 MB, the rule will not trigger for messages of 2 MB and 3 MB and any size in between.

## Headers

- From: contains domain/email address:** Select this option to only include emails from certain domains or email addresses in the report. Click on the **domain/email address** link and select a filter to search for. Alternatively, if you just want to use a one-off email address or domain without having to create a filter, you can enter this in the bottom pane.
- From: is member of group:** Select this option to only include messages from a certain group in the report. Click on the **group** link and check the groups to filter on.
- To: contains domain/email address:** Select this option to only include emails with certain domains or email addresses in the To: field. Click on the **domain/email address** link and select a filter to search for. Alternatively, if you just want to use a one-off email address or domain without having to create a filter, you can enter this in the bottom pane.

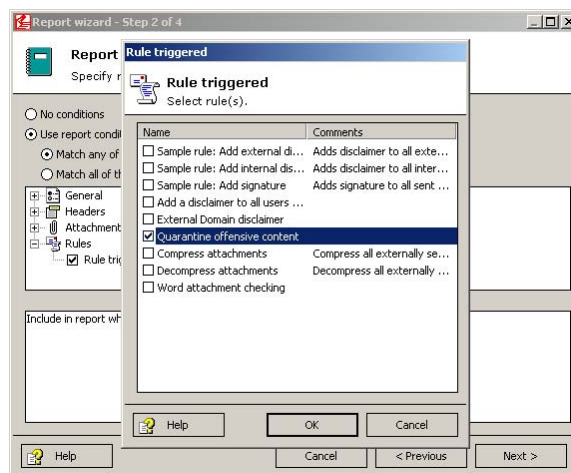
- ☑ **To: is member of group:** Select this option to only include messages with a certain group in the To: field. Click on the **group** link and check the groups to filter on.
- ☑ **Cc: contains domain/email address:** Select this option to only include emails with certain domains or email addresses in the Cc: field. Click on the **domain/email address** link and select a filter to search for. Alternatively, if you just want to use a one-off email address or domain without having to create a filter, you can enter this in the bottom pane.
- ☑ **Cc: is member if group:** Select this option to only include messages with a certain group in the Cc: field. Click on the **group** link and check the groups to filter on.

### Attachments

- ☑ **Attachment exists:** Select this option to only include messages that contain attachments in the report.

### Rules

- ☑ **Rule triggered:** Select this option if you only wish to include messages that triggered certain rules. For instance, you could use this option to create a report on users that triggered the rule 'Quarantine offensive content'.



### Note

Delivery Status Notifications are not included in the reports. Therefore a rule customizing DSNs will never appear as a triggered rule.



4. Specify any report exceptions. If there are no exceptions, click **Next**. If you wish to exclude certain messages from the report, select **Use report exceptions** and select the exceptions that must be met. For instance, you might want to see a report on the amount of messages sent to and from external domains by the Sales department, apart from the head of the sales department. When you are ready, click **Next**.
5. Enter the report name and any comments you have. By default the option **Run report on completion** is ticked. If this is activated the Report generation wizard will pop up after you click **Finish**. For instructions on how to generate reports, see the next paragraph.

## Generating a report

After you have created a report template, you must apply the report to one or more log files and run it to generate an HTML report. To generate a report:

1. If you wish to run a previously created report template, select the report and click **Run**. If **Run report on completion** was ticked, the Report generation wizard will automatically start up after you click **Finish** in the Report wizard.
2. Select the log file(s) to be used for generating the report and click **Add**. If you wish to generate a report on all log files in the list, click **Add all**. For instance, if you wish to see the traffic sent in the month December, select the Monthly log file for 2002/12. Alternatively, if you have enabled daily logging, you can select all December log files. When you are ready, click **Next**.
3. Wait whilst the wizard generates the report. When it is ready you can click **View report**. Internet Explorer will open up and display the report. You can print the report or save it to file. Alternatively enter a name and path in **Report file name** or click on the ... button and browse to a location for storing the file. When you are ready, click **Finish**.

### **Note**

Remember that only the messages that are sent or received by licensed users will appear in the reports.

## Spam blocker

**B**y blocking spam before it arrives at your mail server, Policy Patrol not only saves your users valuable time but also preserves the bandwidth needed for downloading the messages. Policy Patrol includes the option to block messages from any real time spam list you choose.

### Spam lists

There are a number of spam lists that contain IP addresses and domains from known spammers. Policy Patrol can use these lists to identify messages as spam before they are actually downloaded. How accurate this filtering is, depends on the list you use. There are two types of lists:

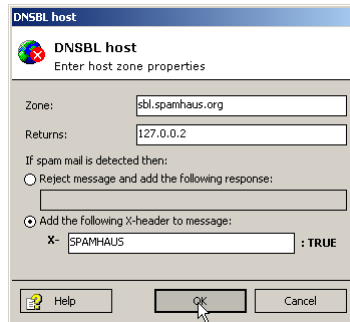
1. Lists of known spammer's domains, for example the [Spamhaus Block List \(SBL\)](http://spamhaus.org/sbl/) (<http://spamhaus.org/sbl/>)
2. Lists of mail servers that are open to relaying and therefore will allow spammers to send mail via their mail server. An example of this last kind of list is the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

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.

### Configuring the spam blocker

To enable the real time spam blocker, tick **Enable real time spam blocker**. To enter a spam list to use, click **Add**. Enter the **Zone** and **Returns** for the list. For instance for the Spamhaus Block List (SBL), enter `sbl.spamhaus.org` for

the zone and 127.0.0.2 for the Returns. To use the Open Relay Database (ORDB) enter `relays.ordb.org` for the zone, and 127.0.0.2 for the Returns.



Policy Patrol can handle spam in two ways: it can reject the message or add an X-header to the message for further processing by a rule.

To reject the message, select **Reject message and add the following response**. If you select this option the message will never reach your mail server and hence will not use any bandwidth. If you wish you can send a response to the sending mail server. For instance 'This mail was rejected by Policy Patrol'. Although this method has many advantages, it is possible that some legitimate emails might be rejected in this way, especially if you are using a list that includes open relays.

Policy Patrol can also add an X-header to the mail to enable you to create rules for these messages. For instance you could add the X-header `X-SPAMHAUS` to all messages originating from spammers on the Spamhaus Block List and then create a rule in Policy Patrol that deletes these messages. To configure this X-header enable the option **Add the following X-header to message** and enter an X-header, for instance `SPAMHAUS`. Now you can specify what Policy Patrol should do with these messages (see the next paragraph for further instructions). When you are ready, click **OK**. You can add as many lists as you wish.

#### **Note**

Deleting messages is not the same as rejecting messages, since messages that are deleted by a rule can still be undeleted in Policy Patrol. However, messages that are rejected by Spam blocker are not even downloaded by your mail server and hence cannot be retrieved. Furthermore, rejected messages do not use any bandwidth, whereas deleted messages do.

## Creating rules for spam messages

To create a rule that processes mails that have been identified by Spam blocker, follow the next steps:

1. Go to Policy rules and click **New**.
2. Select the users for the rule. Click **Next**.
3. Select External messages > **Received**. Click **Next**.
4. Select **Trigger rule if following conditions are met**. Go to **Headers** and select the option **Header of name and value exists**. Click on the link in the description. Enter the X-header that you configured to be added by Spam blocker and enter TRUE as the value. For instance, if you configured Spam blocker to add the X-header SPAMHAUS, enter X-SPAMHAUS as the name and TRUE as the value. Click **OK**. Click **Next**.
5. If you want to set exceptions, select **Do not trigger rule if following exceptions are met**. For instance you can exclude allowed newsletters by going to **Headers** and selecting the option **Sender field contains domain or email address**. Then click on the link and for instance select the sample 'Newsletters' filter (you must still enter your newsletter email addresses in this filter). Click **OK**. Click **Next**.
6. Now select the actions to be taken. You can quarantine, delay, delete or accept the message. Then you can choose any amount of secondary actions, such as sending an email notification, adding a tag, or adding the sender to a filter. For more information on the actions, please consult Chapter 3 Configuring rules. When you are ready, click **Next**.
7. Leave the rule unscheduled and click **Next**.
8. Enter a name for the rule and any comments and click **Finish**.

### Tip

Apart from using real time black lists, Policy Patrol can also search for spam characteristics, such as spam words in the subject or body, spam header characteristics, number of recipients and messages that only contain an HTML body part. To see the different spam detection possibilities, have a look at the sample rule 'Add tag to Spam messages'.

## Virus checking

**P**olicy Patrol includes Kaspersky™ Anti-Virus engine to stop viruses from entering (and leaving) your email system. This chapter discusses the different options that can be configured for virus checking.

### Kaspersky™ Anti-Virus

Kaspersky™ Anti-Virus detects and removes known viruses, even if they are included in compressed, encrypted or archived files. Furthermore, Kaspersky™ Anti-Virus includes a sophisticated Code Analyzer that detects harmful instructions in a code and can therefore block viruses, email exploits and malicious scripts & macros even if they are still unknown. The Code Analyzer has proven to be up to 92% effective. Kaspersky Labs is one of the world's leading developers of data-security software and its virus database is updated twice daily. This ensures that with Kaspersky™ Anti-Virus even the newest viruses can be neutralized quickly. For more information about Kaspersky labs, visit their website at: <http://www.kaspersky.com>.

### Installing Kaspersky™ Anti-Virus

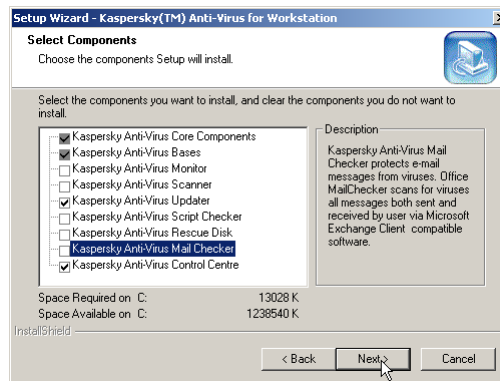
To use Kaspersky™ Anti-Virus you must download and install it on the Policy Patrol machine. Depending on the operating system on the Policy Patrol machine, you need to download Kaspersky™ Anti-Virus for Windows 2000 Professional and Windows XP (<http://www.redearthsoftware.com/files/KAVWinWorkstation.zip>), or Kaspersky™ Anti-Virus for Windows 2000 (Advanced) Server (<http://www.redearthsoftware.com/files/KAVNTServer.zip>).

After you have downloaded Kaspersky, follow the next steps to install it:

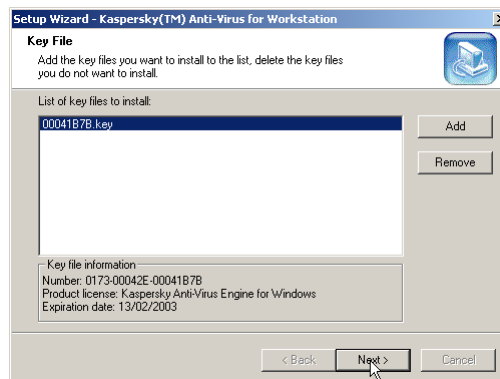
1. In the Welcome screen, click **Next**.
2. Read the License agreement and click **Yes**.
3. Enter your user name and company name. Click **Next**.

## VIRUS CHECKING

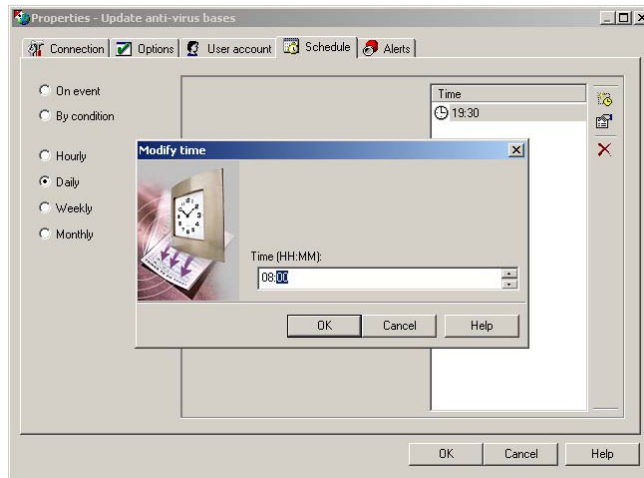
4. Select the installation location for Kaspersky. By default, this is C:\Program Files\Kaspersky Lab\. When you are ready, click **Next**.
5. Enter the program group name in the Start > Programs menu. By default this is Kaspersky Anti-Virus. Click **Next**.
6. In Setup type, select **Custom** and click **Next**. Now select **Kaspersky Anti-Virus Core Components, Kaspersky Anti-Virus Bases, Kaspersky Anti-Virus Updater** and **Kaspersky Anti-Virus Control Centre**. Click **Next**.



7. Review the settings and click **Next** to start copying files.
8. In the Report Viewer Settings screen, select both report viewer associations and click **Next**.
9. Enter the password to be used to remotely access and manage Kaspersky Anti-Virus. Click **Next**.
10. Select the key file in the list and click **Next**.



11. Click **Finish** to exit the installation. Kaspersky will automatically download and apply new anti-virus files daily at 19.30. You can change the scheduling by opening the Kaspersky Anti-Virus Control Centre, right-clicking on **Update anti-virus bases** and choosing **Properties > Schedule tab**.



## Configuring Anti virus

After Kaspersky is installed, open the Policy Patrol Administration console. To enable virus scanning, go to **Anti virus** and check **Enable Kaspersky™ Anti-Virus**. By default Policy Patrol scans all messages for viruses, but if you only want to check certain messages, you can change these options here. You can check outbound, inbound and/or internal messages (internal messages can only be checked if Policy Patrol is installed on an Exchange 2000 machine).

You must also specify what Policy Patrol must do with a message that contains a virus. If you wish Policy Patrol to attempt to clean the virus, select **Attempt to clean virus**. Select **Delete virus if failed to clean** if you wish Policy Patrol to delete the virus if it failed to clean the message. Policy Patrol will only delete the infected attachment or body part. So for instance, if there is a virus found in an attachment that cannot be cleaned, that specific attachment will be deleted. If a malicious HTML script is found that cannot be cleaned, the HTML part of the message will be deleted so that the recipient will receive a plain text version without the script.

### Note

Policy Patrol cannot delete the infected part of an internal message without deleting the entire message. Therefore you must always include a rule that specifies what should be done with internal messages that contain a virus that could not be deleted. In exceptional circumstances it is also possible that Policy Patrol cannot delete a virus from an external message. It is recommended to configure a rule that specifies to for instance delete or quarantine all messages that contain a virus that could not be deleted.

## Configuring rules for virus checking

To configure a rule that processes mails with viruses, for instance to notify the sender that their message has been deleted, or to add the sender's email address to a 'Virus senders' filter, create a new rule and check the condition **Message contains virus**. Click on the **contains virus** link and select one or more options. You can then configure actions to be taken with these messages. Cleaning the virus must be configured from the Anti-virus tree node. This cannot be configured in a rule.

For instance, to create a rule that quarantines all messages with viruses that cannot be cleaned or deleted:

1. Go to **Policy rules** and click **New....**
2. In the Users dialog, select that the rule should apply to **All users**. Click **Next**.
3. Check **Sent** and **Received** for Internal messages and **Sent** and **Received** for External messages. Click **Next**.
4. Enable **Trigger rule if following conditions are met**. In General, select **Message contains virus**. Click on the **contains virus** link and select **Message contains virus that could not be cleaned** and **Message contains virus that could not be deleted**. Click **Next**.
5. Leave **No exceptions** enabled. Click **Next**.
6. Select **Quarantine message** as the primary action. Click on the **quarantine message** link. In the Reject notification tab, tick Sender and select **Your message has been deleted**. Enable **Send notification** and check Sender's manager. Select the template **Virus sent** from the list. Click **Next**.
7. Leave **No scheduling enabled**. Click **Next**.
8. Enter 'Quarantine viruses that could not be deleted or cleaned' as the rule name, leave **Enable this rule** and **Process following rule(s)** checked and enter the following comments: 'This rule quarantines all internal messages that include viruses'. Click **Finish** to create the rule.

### Tip

It is advisable to activate the sample rule **Quarantine viruses that could not be deleted**, since otherwise the occasional virus could still get through.



## Advanced options

**P**olicy Patrol includes some advanced options that can be configured from server name > Properties. This includes system directories, code pages, spoofed attachments, local domains and system parameters.

### General

The General Tab provides an overview of your Policy Patrol installation. It lists the computer name and IP address of the Policy Patrol machine and the domain in which it is installed. Furthermore, the Policy Patrol version number, installation type and installed components are displayed.

### Local domains

This tab shows a list of the local domains and excluded IP addresses.

#### **Add and remove local domains**

Policy Patrol uses the local domains list to determine which emails are internal or external. Messages sent from a local domain to a non-local domain qualify as an externally sent message. Messages sent from a non-local domain to a local domain qualify as an externally received message. Messages sent between local domains are classed as internal messages. During installation Policy Patrol asks you to enter your local domain(s). If you need to change these you can add or remove the local domain(s). To add a domain, click **Add...** and enter the domain, for instance `redearthsoftware.com`. Click **OK**. You can remove domains by selecting a domain and clicking **Remove**.

#### **Auto detect local domains**

To retrieve the new local domains automatically, click on **Auto detect**. Specify whether you wish to use the default domain controller or enter the domain controller name or IP address in **Use the following domain controller**. Click **Next**. Policy Patrol will display all the local domains for the domain controller. Click **Finish** to add the local domains to the list. Finally, select 'Yes' if you wish the existing domains in the list to be deleted, or select 'No' if you wish to add

the new local domains to the existing ones. Remember that Policy Patrol can only auto detect if you have Active Directory installed.

#### **Exclude IP addresses**

This list includes IP addresses that Policy Patrol should exclude from processing. This can be useful if you have more than one Policy Patrol installation and you wish to exclude mails originating from another Policy Patrol installation. To add an IP address, click **Add**. Enter the IP address and click **OK**. To remove an IP address from the list, select it and click **Remove**.

## System directories

In this tab you can edit the locations for the queue, work, quarantined, delayed and deleted messages directory. To change the location, edit the path or click on the ... button and browse to the right directory.

## Message flow logging

Message flow logging is used for creating reports. By default, message flow logging is enabled and the log is stored in C:\Program Files\Red Earth Software\Policy Patrol\Log\MsgFlow. You can disable message flow logging or change the location for storing the log. You can also select whether to log periodically. By logging periodically, Policy Patrol will create a new log file each day, month or quarter. If you select daily, the following suffix will be added to the file name: *Dyyyymmdd*, e.g. MSGD20020926. If you select monthly the following suffix will be added: *MyYYmm*, e.g. MSGM200209. The following suffix will be added if you select Quarterly: *Qyyyyq*, where q stands for the quarter. For instance MSGQ20023 is the archive for the 3<sup>rd</sup> quarter of 2002. If you do not enable archive periodically, the complete log will be kept in one file. The file will include the suffix *u*, e.g. MSGU.

#### **Note**

Remember that if you do not enable message flow logging you will not be able to create reports.

## System logging

In this tab you can edit the options for system logging. You can edit the directory where the system logs are kept and you can select whether to log periodically. By logging periodically, Policy Patrol will create a new log file each day, month or quarter. If you select daily, the following suffix will be added to

the file name: Dyyyyymmdd, e.g. LogD20020926. If you select monthly the following suffix will be added: Myyyyymm, e.g. Log200209. The following suffix will be added if you select Quarterly: Qyyyyyq, where q stands for the quarter. For instance LogQ20023 is the archive for the 3<sup>rd</sup> quarter of 2002. If you do not enable archive periodically, the complete log will be kept in one file. The file will include the suffix U, e.g. LogU. Finally, you can specify whether Policy Patrol errors should also be written to the Windows event log viewer.

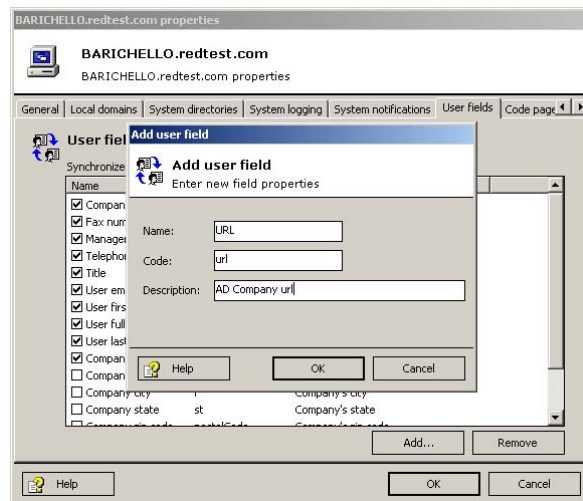
## System notifications

In this tab you can specify the options for system notifications. In the From: field, enter the sender of the email. The sender must be an existing internal email address. In the To:, Cc: and Bcc: fields, enter the recipients for the system notifications. For internal recipients you can also click on ... and select the recipient from the user list. The recipient addresses entered here will also be taken as the Administrator address(es) when configuring notifications.

## User fields

Policy Patrol already includes a number of merge fields taken from Active Directory, Exchange 5.5 or Lotus Domino. If you wish to add more fields, click **Add...** Enter the **name** of the field and the **code**. Enter a **description** and click **OK**. Remember that each time you add a user field you must run the Connector so that Policy Patrol can retrieve the user information for the field.

Each time Policy Patrol synchronizes, the program will pick up all these fields for each user. If you are not going to use certain fields, it might be wise to remove these fields from the list in order to increase the speed of synchronization. To remove a field, select the appropriate field and click **Remove**.



## ADVANCED OPTIONS

Remember that each Connector type will use a different field code. For instance, the Active Directory uses the 'url' code to identify the company's home page. However, this might not be the same for Exchange server 5.5 and Lotus Domino. Therefore, if you have connectors that retrieve users and fields from different mail servers and you are adding user fields, enter the directory type in front of the field, e.g. AD for Active Directory, to distinguish it in the list.

The tables below list several codes that can be used for Exchange server 5.5 and Lotus Domino.

Description	Exchange 5.5 directory code
User's display name	cn
User's first name	givenname
User's last name	sn
User's initials	initials
User's email address	mail
User's department	department
User's phone number	telephoneNumber
User's second phone number	telephone-office2
User's fax number	facsimileTelephoneNumber
User's mobile number	mobile
User's pager number	pager
User's home phone number	homephone
User's office location	physicaldeliveryofficename
User's job title	Title
User ID	uid
User's Assistant	secretary
Company name	company
Company's address	postalAddress
Company's city	l
Company's state	st
Company's zip code	postalCode
Company's country	co

Description	Lotus Domino directory code
User's full name	cn
User's first name	givenName
User's last name	sn
User's suffix	generationQualifier
User's email address	mail
User's phone number	telephoneNumber
User's fax number	facsimileTelephoneNumber
User's mobile number	mobile
User's personal title	personalTitle
User's job title	title
User's home phone number	homePhone
Company's address	postalAddress
Company's city	l

Company's state	st
Company's zip code	postalCode
Company's country	c
Company's url	url

## Code pages

By default, Policy Patrol content checks all code pages. It is also possible to exclude certain code pages for content checking. You can do this if for instance you receive messages with characters that do not exist in the English language and you do not wish to content check these particular characters. To exclude a code page, click **Add...** enter the code page name and click **OK**. You can also configure Policy Patrol to only content check certain code pages. To do so, activate the radio button **Content check only code pages selected below:**. Then check the code pages to content check.

## Attachment checking

This tab includes the option to enable/disable Microsoft Word attachment checking. By default this feature is disabled. If you wish to enable Microsoft Word content checking, you must select **Enable Microsoft Word content checking** and install Microsoft Office XP (Word only) on the Policy Patrol server machine.

## Attachment spoofing

This tab lists the file types that Policy Patrol can verify the extensions of. Policy Patrol can verify over a 100 file types. For instance, if a user tries to circumvent a rule blocking exe files and renames the `virus.exe` file to `virus.doc`, Policy Patrol will be able to verify that the file is not a doc file. If there are any files that you wish to add to the list, you can send three examples of the file type to [development@reearthsoftware.com](mailto:development@reearthsoftware.com). If it is possible to verify the file type, we will email you back a file that you can import so that Policy Patrol will be able to verify the file type.

## Delivery notifications

This tab lists the Delivery Status Notifications that Policy Patrol can customize. Most notifications are already added, but if you need to add further notifications, you can do so by clicking on **Add...** Select whether it is a Success, Delay or Failure notification. Enter the DSN code and a description. Click **OK** to add the notification. If you wish to remove a notification from the list, select the notification and choose **Remove**.

## **Advanced**

This tab lists the Policy Patrol system parameters (similar to registry keys). Normally you do not need to make any changes in the system parameters unless you are asked to do so by Policy Patrol technical support staff.

## Sample rules

**P**olicy Patrol includes several sample rules to help you enforce your email policy as soon as possible. You can use the sample rules as they are, adjust them, or make your own rules. The program also includes some sample filters and templates that are not used in the sample rules.

### Delete messages from the Spam senders filter

This rule applies to all externally received messages and deletes messages that are sent from domains in the **Spam senders** filter, except if the domain or email address is listed in the **Exclude from Spam senders, Newsletter** or **Automatic white list** filter. Policy Patrol adds the sender domain to the Spam senders filter each time a message triggers the rule 'Add tag to spam messages'. Since the recipient first sees the message with the spam tag, the user can warn the Administrator if the message was wrongly identified as spam. The Administrator must then either add the domain to the **Newsletter** filter or to the **Exclude from Spam senders** filter. The Exclude from Spam senders filter includes domains such as hotmail.com and yahoo.com. This is because some spammers pretend to send their messages from these domains, and you would probably not want to delete all messages from these domains. Finally, the automatic white list includes a list of all domains that users have sent emails to, and therefore cannot be spam senders.

**Required:** Enable the rule. For the rule to work, you must also enable the rules 'Add tag to spam messages' and 'Automatically create white list'.

**Optional:** Instead of deleting you could add a tag, or quarantine the mails. You can add more domains to exclude in the **Exclude from Spam senders** and **Newsletter** filter. Tip: If you want to give your users two chances to add an address to the **Newsletter** or **Exclude from Spam senders** filters (i.e. to avoid these messages from being deleted), you can first add spammers to a **Spam senders 1** filter. If they send another spam message, add the sender to **Spam senders 2** filter. Then change this rule to delete all mails from **Spam senders 2** filter. If you are not sure how to create these rules, you can use the rules **Delete all mails from re-offending virus senders** and **Add re-offending virus senders to filter** as an example.

## Delete all mails from re-offending virus senders

This rule checks all externally received mails. If a mail is sent by a sender in the **Re-offending virus senders** list, the mail is deleted and the sender is notified that the message has been deleted. The Re-offending virus senders list contains email addresses of senders of at least two viruses.

**Required:** Enable the rule. For the rule to work, you must also enable the rules 'Notify when virus is cleaned or deleted' and 'Quarantine viruses that cannot be deleted'. Enter the company telephone number in the **Re-offending message deleted** template.

**Optional:** Instead of deleting you could add a tag, or quarantine the mails. You can customize the template **Re-offending message deleted**.

## Delay large messages

This rule applies to all external messages and delays the delivery of mails larger than 10 MB until after 6 pm. The size includes the message body and all attachments. When the mail is delayed, the sender receives the notification **Your message has been delayed**.

**Required:** Enable the rule.

**Optional:** You can exclude certain users from this rule and increase or decrease the message size condition. Furthermore, you can change the time of delivery and the notification template **Your message has been delayed**.

## Add re-offending virus senders to filter

This rule applies to all messages and triggers if the sender is from the **Virus senders** list and the message includes a virus. If both conditions are met, the sender's email address will be added to the **Re-offending virus senders** list.

**Required:** Enable the rule.

## Quarantine viruses that cannot be deleted

In Policy Patrol > **Anti virus** you can configure the options for virus checking. Policy Patrol can detect and attempt to clean all viruses that pass through it. If a virus cannot be cleaned, Policy Patrol can try to delete it. However, Policy Patrol is not able to delete the virus if this means deleting the whole message, which is the case for internal messages, and possibly for an external message with an infected attachment and no message body. To make sure that the messages with viruses that could not be deleted do not get through, this sample rule is included. The rule checks all messages for viruses that could not



be deleted and quarantines them. The Administrator will receive an email notification and network message that an email with a virus has been quarantined and the sender email address will be added to the **Virus senders** filter. If the mail is rejected, the sender will receive notification of this.

**Required:** Open the rule properties and click on the **send network message** link. In the **To** field enter the IP address of the Administrator's machine for sending the network message. Enable the rule.

**Optional:** You can customize the templates **Undeleted virus quarantined** and **Message with virus deleted**.

 **Note**

Remember that Policy Patrol can only check internal messages if it is installed on an Exchange 2000 machine.

## Quarantine suspected viruses

This rule applies to all messages and quarantines messages with suspected viruses or password protected attachments that could not be scanned. When a message is quarantined the Administrator receives a notification message. If the message is rejected, the sender receives a notification email.

**Required:** Enable the rule.

**Optional:** You can edit the notification messages **Suspected virus quarantined** and **Message with suspected virus deleted**.

## Quarantine all scripts

This rule checks all messages and quarantines mails that contain HTML scripts in the message body and/or HTML attachment(s). The Administrator will receive notification when messages are quarantined so that they can be checked for malicious content. The Administrator can then decide to accept or reject the message. The Administrator can also decide to remove the HTML version of the mail and deliver it in plain text instead, or to remove a particular attachment.

**Required:** Enter the company telephone number in the **Script sent deleted** template. Enable the rule.

**Optional:** You add more script tags to the **Script tags** filter and customize the notification templates **Script sent quarantined** and **Script sent deleted**

and instead of quarantining scripts, convert all mails that contain scripts to plain text. You can also exclude certain users from the rule.

## Quarantine offensive content

This rule applies to all mails and quarantines messages that include offensive content in the message subject, body or attachment. A notification is sent to the recipient's and sender's manager to view and accept or reject the mail. If the mail is rejected the sender receives a notification.

**Required:** Enter the company telephone number and email address in the **Inappropriate mail deleted** template. If you wish to check Word documents you must enable Microsoft Word checking in server name > Properties > **Attachment checking** and install Microsoft Office XP on the server machine. Enable the rule.

**Optional:** You can customize the **Offensive content** word/phrase filter and apply the rule to certain users. Furthermore, you can customize the notification templates **Inappropriate mail sent**, **Inappropriate mail received** and **Inappropriate mail deleted**. For internal mails, two managers will receive a notification. If you do not wish this to happen, you can make one rule for external messages and configure a notification to be sent to the sender's and recipient's manager. Then create another rule that checks internal messages and only sends a notification to either the sender's or recipient's manager. Tip: You can attach your email policy to the reject email.

## Block dangerous attachment types

This rule applies to all messages and quarantines attachment types that might contain viruses or harmful scripts. A notification is sent to the Administrator to view and accept or reject the mail. If the message is rejected, the sender will receive a notification message.

**Required:** Enter the company telephone number in the **Dangerous attachment type deleted** template. Enable the rule.

**Optional:** You can customize the **Dangerous attachment types** filter and exclude certain users from the rule. Furthermore you can customize the templates **Dangerous attachment type quarantined** and **Dangerous attachment type deleted**.

## Block spoofed attachments

This rule checks all attachments for spoofing. It checks for multiple extensions, CLSID extensions, binary files that have been disguised as text files, and it will attempt to verify the attachment extension. If the attachment is spoofed, the

## SAMPLE RULES

message will be quarantined and a notification is sent to the Administrator to review the message, and to the sender to inform them that the message is under review. If the message is deleted, the sender will receive a notification message.

**Required:** Enable the rule.

**Optional:** You can customize the templates **Spoofed attachment quarantined**, **Spoofed attachment sent** and **Spoofed attachment deleted**.

## Notify when virus is cleaned or deleted

This sample rule applies to all messages and notifies the Administrator, sender and recipient that a virus was found and successfully removed. Finally, the sender is added to the **Virus senders** Email addresses/domains filter.

**Required:** Enable the rule.

**Optional:** You can customize the notification templates **Virus cleaned/deleted**, **Removed virus sent**, and **Removed virus received**.

## Add signature

This rule applies to all sent messages and adds a signature after the last entered message text.

**Required:** Enter your URL in the **Signature** template. Enable the rule.

**Optional:** You can customize the signature by going to **Templates > Disclaimer** and double-clicking on the **Signature** template. Tip: Do not enter too much text in the Signature Word/Phrase filter since this will require more processing time.

## Add external disclaimer

This rule adds a disclaimer to every externally sent message, except if [No disclaimer] is found in the subject. In this way, users will be able to disable a disclaimer for a particular email by entering [No disclaimer] in the subject. The [No disclaimer] entry is then removed from the subject by the rule Remove [No disclaimer] from the subject. The rule prevents adding multiple disclaimers when replying or forwarding by searching the body for part of the disclaimer text. If it finds the text, it will not add the disclaimer again.

**Required:** Enable the rule. Enable the rule Remove [No disclaimer] from the subject.

③ **Optional:** You can customize the disclaimer text by going to **Templates > Disclaimer** and double-clicking on the **External disclaimer** template. It is a good idea to include your company name in the **External disclaimer** filter along with a few words from your disclaimer to make sure the exclusion applies to your company's disclaimer as opposed to the sender's or recipient's disclaimer. Remember that if you change the disclaimer text you must also change the **External disclaimer** Word/Phrase filter. Tip: Do not enter too much text in the External disclaimer Word/Phrase filter since this will require more processing time.

## Add internal disclaimer

This rule adds a disclaimer to every internally sent message. It prevents adding multiple disclaimers when replying or forwarding by searching the body for part of the disclaimer text. If it finds the text, it will not add the disclaimer again.

**Required:** Enable the rule.

③ **Optional:** You can customize the disclaimer by going to **Templates > Disclaimer** and double-clicking on the **Internal disclaimer** template. Remember that if you change the disclaimer text you must also change the **Internal disclaimer** Word/Phrase filter. Tip: Do not enter too much text in the Internal disclaimer Word/Phrase filter since this will require more processing time.

## Automatically create white list

This rule applies to externally sent messages and adds the To: domain to the **Automatic white list** filter every time a user sends out an email. This filter is then used as an exception in the 'Add tag to Spam messages' and 'Delete messages from Spam senders filter' rules.

**Required:** Enable the rule.

## Add tag to spam messages

This rule applies to externally received messages and adds the tag 'SPAM:' to messages that:

- Include spam header characteristics.
- Are detected as spam by the real time Spam blocker.
- Include spam words in body and/or subject.
- Have more than 15 recipients.

In addition to adding the tag, the rule adds the senders' email addresses to the **Spam senders** Email addresses/domains filter. If another message is received from the same sender, the message will be deleted by the rule 'Delete messages from the Spam senders filter'. Advise your users that if a message is tagged wrongly as spam (this happens with newsletters for instance), they should ask the Administrator to add the from: email address to the **Newsletter** or **Exclude from spam senders** filter so that it no longer gets tagged as spam and it does not get deleted. In this way, the possibility of wrongly deleting emails is minimized. Furthermore, the 'SPAM:' tag will not be added if the sending domain is listed in the **Automatic white list** filter, which includes a list of all domains that users have sent emails to.

**Required:** Enable the rule and add the from email addresses of allowed newsletters to the **Newsletter** filter. Configure the spam blocker: Tick **Enable real time spam blocker**. Click **Add** and enter the **Zone** and **Returns**. For instance for the Spamhaus Block List (SBL), enter `sbl.spamhaus.org` for the zone and `127.0.0.2` for the Returns. Select **Add the following X-header to the message** and enter `SPAMHAUS` as the X-header. Click **OK**. Finally, enable the rule 'Automatically create white list'.

**Optional:** You can customize the **Spam words** filter, add or remove spam characteristics, and increase or decrease the number of recipients condition. Furthermore you can choose to delete the messages, rather than adding a tag and then deleting the message if sent from the Spam senders list.

### Tip

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. Since each message contains a unique ID, the spammer will know exactly which recipient has viewed the mail. In this way, spammers know how many people have viewed their message and which email addresses are still 'live'.

To block these messages, create a rule in Policy Patrol that applies to all users and externally received messages. In conditions, go to **General** and select **Message is of format**. Click on the **format** link and select **HTML**. Click **Next**. In exceptions, go to **General** and select **Message is of format**. Click on the **format** link and select **Plain text**. Go to **Headers** and select **Sender field contains domain or email address**. Select a filter of allowed newsletters and any other white list you would like to exclude from the rule. When you are ready, click **Next**. Specify whether you wish Policy Patrol to

Quarantine, Delay, Delete or Accept the message. If you wish you can select secondary actions. Click **Next**. Configure scheduling if necessary and enter the name for the rule. Click **OK**.

## Customize Delivery Status Notifications

This rule applies to all internally sent Delivery Status Notifications (DSN) (from postmaster) and customizes DSN 4.4.7, 5.1.1, 5.5.0 and 5.7.1.

**Required:** Select the postmaster account as the user and enable the rule.

**Optional:** You can customize the templates DSN 4.4.7, 5.1.1, 5.5.0 and 5.7.1. You can also customize externally sent DSNs by applying the rule to externally sent messages as well as internally sent messages.

## Remove [No disclaimer] from the subject

This rule applies to all messages and removes '[No disclaimer]' from the subject. Users can enter this in the subject if they want to disable a disclaimer for a particular mail. This rule will then remove [No disclaimer] from the subject so that the recipient will not see it.

**Required:** Enable the rule.

**Optional:** You can change the [No disclaimer] code and filter if you wish.

## Compress attachments larger than 1 MB

This rule applies to all external messages and compresses the attachment(s) if a message is found with an attachment larger than 1 MB.

**Required:** Enable the rule.

**Optional:** You can change the comment for the newly created zip file, and you can select to compress each attachment in a separate file. Furthermore, you can change the attachment size that triggers the rule.

## Archive all mails

This rule archives all messages into the monthly **Default Archive**.

**Required:** Enable the rule.

## SAMPLE RULES

③ **Optional:** In the **Default Archive** properties, you can change the path where the XML file is saved. By default this is C:\. You can also create a new archive that is saved in csv or xml format and is created daily, monthly or quarterly. You can select the fields to be included in the archive. Finally, you can apply the archive rule only to certain users or customers and add a billing code.

## Troubleshooting

**T**his chapter deals with Policy Patrol troubleshooting. If you have a problem you can consult the System Events in the program, the Policy Patrol online knowledge base, or request support from Red Earth Software by running the Support Wizard.

### System Events

If something is not working as it should, check the **System Events** in Policy Patrol to see if there are any errors. If there are any errors these might point you in the right direction.

### Knowledge Base

If you have a question or problem with Policy Patrol you can consult our extensive online knowledge base at <http://www.policypatrol.com/kb.asp>. Some of the questions and answers are listed below. If you do not find your answer, please send an email to [support@reearthsoftware.com](mailto:support@reearthsoftware.com).

#### **Will Policy Patrol search embedded emails?**

Yes, Policy Patrol will apply word/phrase conditions to any amount of embedded emails and to any level. For instance, if you wish to block the word 'confidential' in an email's subject and you receive a message within a message that contains this word in the subject, it will be blocked. This will also be the case for words/phrases in the body or attachment, attachment type and attachment name.

#### **User field is not working**

There can be several reasons why a user field is not replaced with merge information:

- Verify that the code for the field is correct. Some default fields include codes that are only applicable to Active Directory. For instance, in Exchange 5.5 the fields 'Company street' and 'Company P.O. Box' have different codes than Active Directory. If you want to use the Company



street field for Exchange 5.5, go to server name > Properties > User fields tab. Click **Add**. Enter a name and `PostalAddress` as the code. Click **OK** to save the field.

- ☑ If the code is correct, check whether there is anything entered for the appropriate field in Active Directory Users and Computers > User Properties. If it is an Exchange 5.5 or Lotus Domino field, verify that information is entered in the Exchange/Lotus Domino mailbox properties for the user. If there is nothing entered, you must enter the information and run the respective connector to retrieve the information.
- ☑ Check the field in the Template to see whether you might have applied formatting to part of the field. If you don't select the whole field this will cause the fields not to be replaced.
- ☑ You must run the connector after adding a new field in server name > Properties > User fields and after updating information in the Active Directory, Lotus Domino or Exchange 5.5 mailbox properties.

#### **My disclaimer attachment is empty**

If you selected **Add disclaimer as plain text attachment**, and the attachment is empty, this is because there is no text in the RTF/plain text tab of the template. Open the template properties and whilst the HTML tab is selected, click on the far right button, **Copy to...** Click **OK** and choose **Commit** to save the changes. Now the disclaimer text will be copied to the RTF/plain text tab and the attachment will contain your disclaimer text.

#### **My rule that searches for words/phrases always triggers**

Check whether you have enabled word score in the selected Word/Phrase filter, and have left the word score threshold in the rule at 0. In this case all messages will reach the word score 0, and hence the rule will always trigger.

#### **Why is the message size not the same as in Outlook or Quarantined items?**

Policy Patrol counts the actual message size as received by the mail server. This can be a little different from the message size as received by Outlook or the message size of a Quarantined message in Policy Patrol. There are a number of reasons for this, such as different encoding of the email or attachment, or the method of determining the size. Policy Patrol looks at the size as received by the mail server since this is the size that will use actual bandwidth, whereas the size as specified in Outlook indicates storage space. Moreover, a quarantined message is encoded differently from a message that passes through the mail server.

#### **How do I enable remote administration after installation?**

If you did not select **Enable Remote Administration** during installation, you must start the service `PP2_RemoteManager` and set it to **Automatic**. Go to Start > Programs > Administrative Tools > Services > double-click on `PP2_RemoteManager`. Set the Startup type to **Automatic**. Click **OK**. Right-click on the `PP2_RemoteManager` service and select **Start**. Now install the

Administration Console on the remote machine and you will be able to configure Policy Patrol remotely.

**Inline pictures are treated as attachments**

By default, Policy Patrol will treat inline pictures as attachments. This means that pictures in HTML messages are included for the conditions **Attachment exists**, **Number of attachments**, **Remove attachment(s)**, and **Attachment is of size**. Policy Patrol counts inline pictures for security reasons, since inline pictures can include viruses. If you do not want inline pictures to be counted as attachments, this can be changed by a system parameter. Please contact [support@redearthsoftware.com](mailto:support@redearthsoftware.com) for instructions on how to do this.

**Can I undelete deleted messages?**

Yes this is possible. Go to **Monitoring > Deleted**. Select the appropriate message and click **Undelete**. The message will now be delivered.

**Can Policy Patrol retrieve Exchange 5.5 distribution lists?**

Yes, Policy Patrol retrieves Exchange 5.5 users and distribution lists. In addition, Policy Patrol retrieves Exchange 5.5 mailbox properties for the user merge fields.

**Will Policy Patrol automatically retrieve and license new users?**

Yes, if you select **License users automatically** when creating the connector, new users are automatically licensed in Policy Patrol upon synchronization. However you must make sure that you have enough Policy Patrol licenses since if this is not the case, Policy Patrol will randomly license your users.

**I can no longer see the tree nodes Monitoring, Reporting, Archiving, Anti-virus and Spam blocker**

This is because you have either deleted all your serial numbers, or you have entered a serial number for Policy Patrol Disclaimers. If you wish to use these features, you must purchase a serial number for Policy Patrol Enterprise.

**Are attachment names case sensitive?**

No, the names in the Attachment Name filter are not case sensitive. So if you create a filter with the attachment name love-letter-for-you.vbs, Policy Patrol will also apply the filter when LOVE\_LETTER\_FOR\_YOU.vbs is found.

**I have not made any changes but still Policy Patrol asks to commit changes**

Each time you click **OK** instead of **Close** or **Cancel** in a dialog, Policy Patrol will presume that you have made changes. Therefore once you have clicked **OK**, a \* will appear after your server name, and Policy Patrol will ask whether you wish to commit your changes when you close the Administration console.

**I cannot enable my rule**

This happens when you still need to configure one or more option(s). Open the rule properties and click on the red links in the description to select the required options.

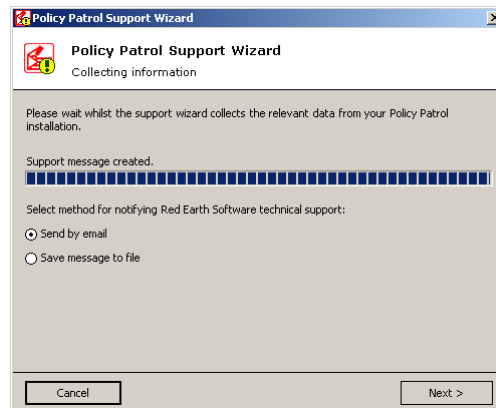
**Can Policy Patrol also check email addresses in the bcc: field?**

Yes, if you select the condition **Receiver fields contain domain/email address**, Policy Patrol will also check the email addresses and domains entered in the bcc: field.

## Support Wizard

If you are experiencing a problem with Policy Patrol, you can use the Policy Patrol Support Wizard to gather all the relevant information and send a message to Red Earth Software technical support. To run the Support Wizard:

1. Go to Help > Support Wizard. The Support Wizard will start up.
2. In the Welcome screen, click **Next**.
3. Enter your contact information and Maintenance ID if available. Make sure that you describe your problem in as much detail as possible, giving steps to reproduce the problem where possible.
4. The Wizard will now collect the relevant information and prepare the message for Red Earth Software technical support. When ready, you will be able to select how to notify technical support. If you select **Send by email** the wizard will email the message to technical support. If you select **Save message to file** you will be asked to specify a location for storing the file, and the message will be saved as an .eml file. To send the message, double-click on the file. The message will be opened in Outlook Express. Click **Send** to send the message to Red Earth Software technical support.



5. Depending on your previous selection, the screen **Message Sent** or **Message Saved** will pop up. Click **Finish** to exit the wizard.

# Index

---

## A

Accept message · 76  
Actions · 43  
Active Directory · 19, 23, 24, 60, 64, 66, 67, 96, 97, 111  
Add attachment · 46  
Add business card · 47  
Add From: domain/email address to filter · 48  
Add To: domain/email address to filter · 49  
Administrator address(es) · 97  
Archive message · 32, 45, 48, 54, 59, 64, 78, 79, 80, 81, 96, 97  
Attachment contains word/phrase · 41  
Attachment exists · 40, 112  
Attachment name · 41, 51, 54, 58, 82, 110, 112  
Attachment Name Filter · 58  
Attachment size · 40, 112  
Attachment type · 41, 59, 74, 110  
Attachment type filter · 59

---

## B

Backend Exchange server · 12  
Billing code · 48, 81  
Binary text file · 42  
Body · 32, 40, 70, 80, 83  
Bold · 63

---

## C

Case sensitive · 56, 57, 58, 112  
Change Order · 55  
Change priority/importance · 48  
Clean virus · 93  
CLSID extension · 41  
Clustering · 8  
Commit changes · 22, 53, 111  
Compress · 46  
Conditions · 32

Connector · 19, 20, 23, 24, 25, 26, 27, 60, 67, 112  
Convert to plain text · 48  
CSV archive · 78

---

## D

Date/Time fields · 70  
Decompress · 47  
Default connector · 20  
Default value · 64, 66  
Delay message · 43, 54  
Delayed · 72  
Delete message · 44  
Delivery receipt request · 35, 48  
Delivery Status Notification · 35, 49  
Digitally signed · 33  
Disclaimer · 26, 45, 46, 51, 54, 55, 65, 67, 105, 106, 111  
Domain controller · 19, 24, 95  
Domain/Email address filter · 59  
DSN fields · 69

---

## E

Encrypted · 33  
Event Log · 50  
Exceptions · 26, 30, 42, 43, 54, 81, 94  
Exchange 2000 · 7, 12, 17, 19, 20, 23  
Exchange 5.5 · 7, 19, 23, 25, 64, 66, 67, 97, 111, 112  
Exclude IP addresses · 18  
Export · 57, 58, 59, 60, 63, 66  
External messages · 4, 18, 35, 69, 73, 74, 95, 102, 105

---

## F

False positives · 32, 88  
FAQs · 110  
Field prefix · 64, 66  
Font color · 63

Font size · 63  
Font type · 63  
Frequently asked questions · 110  
Frontend Exchange server · 12

---

## **H**

HTML format · 49, 67  
HTML source · 40, 41, 63, 65, 73, 77  
HTTP · 23

---

## **I**

Import · 57, 58, 59, 60, 63, 66  
Inline HTML pictures · 40, 42, 46  
Insert Field · 62, 66  
Insert image · 63, 66  
Installation · 7, 15  
Internal messages · 4, 7, 8, 12, 18, 19, 34, 47, 48, 69, 73, 74, 93, 94, 95, 97, 102, 106  
Italics · 63

---

## **K**

Kaspersky · 91  
Knowledge Base · 110

---

## **L**

License users automatically · 25, 26, 112  
Local domains · 18, 95  
Logging · 82  
Lotus Notes · 8  
Lotus Notes/Domino · 6, 8

---

## **M**

Match all of the conditions · 32, 84  
Match any of the conditions · 32, 84  
Message date · 34, 84, 85  
Message fields · 68, 70, 80  
Message format · 35  
Message priority · 34  
Message sensitivity · 34  
Message size · 34, 85  
Microsoft .NET Framework · 6, 13, 22  
Monitoring · 26, 44, 72, 76, 112  
Multiple extensions · 41, 104

---

## **N**

Network message · 45  
Notification message · 27, 35, 43, 44, 49, 51, 62, 63, 69, 70, 75, 76, 77, 94, 99, 102, 103, 104, 105  
Number of attachments · 5, 42  
Number of recipients · 37

---

## **O**

On hold · 72  
Open Relay Database (ORDB) · 89  
Ordering · 51, 52, 53, 54, 55  
Outlook Web Access · 12

---

## **P**

PGP · 33  
Policy Patrol Configuration Wizard · 17  
Policy Patrol Disclaimers · 26  
Policy Patrol Enterprise · 26  
POP3 clients · 12  
Port · 21, 23  
Primary actions · 43  
Print message · 47  
Process following rule(s) · 52, 54, 81, 94  
Processing time · 54, 105, 106

---

## **Q**

Quarantine message · 43, 54, 94, 101, 102  
Quarantine remarks · 69, 75, 76

---

## **R**

Read receipt request · 35, 48  
Real time spam blocker · 88  
Receiver field contains domain or email address · 37  
Reject message · 76, 94  
Remote administration · 5, 21, 22, 28, 70, 111, 112  
Remote Administration · 111  
Remove attachment · 46, 112  
Rename · 53, 60, 67  
Replace words/phrases in subject · 47  
Report types · 83  
Reporting · 82  
Reports · 82  
Restore deleted message · 76  
RTF/plain text · 46, 65, 111  
Rule fields · 70  
Rule scheduling · 51

---

## **S**

S/MIME · 33  
Scheduling · 25, 81, 94  
Secondary actions · 43, 44, 51, 54, 55  
Send blind copy · 44  
Sender field contains domain or email address · 37  
Services · 28  
SMTP service · 12  
Spam characteristics · 38, 48  
Spamhaus Block List (SBL) · 88, 107  
Spoofed attachment · 41, 95, 104  
SQL Server · 78

---

Subject · 32, 39, 55, 69, 72, 73, 80  
Support Wizard · 113  
System Events · 110  
System logging · 96  
System parameters · 95, 100  
System requirements · 6

---

## **T**

Tag · 40, 41, 45, 51, 55, 64, 101, 102, 106, 107  
Tag template · 64  
TCP · 21, 23  
Templates · 26, 62, 65, 67, 70, 102, 104, 105

---

## **U**

Underline · 63  
Update wizard · 7, 27, 28  
User fields · 67, 97  
Users · 8, 19, 20, 23, 24, 25, 26, 27, 30, 37, 38,  
45, 54, 80, 88, 94, 102, 104, 105, 107, 112,  
113

---

## **V**

VCard · 47  
Verify attachment extension · 42  
Virus · 26, 36, 41, 42, 69, 91, 93, 94, 99, 102,  
103, 105, 112

---

## **W**

Web monitor · 76, 77  
White list · 42  
Whole or part of word(s) are matched · 57  
Whole word(s) are matched · 57  
Windows 2000 · 6  
Word score · 32, 33, 40, 56, 57, 111  
Word score threshold · 32, 33, 40, 56, 57, 111  
Word/phrase filter · 33, 39, 40, 41, 104  
Word/Phrase filter · 56, 106, 111

---

## **X**

X-Header · 38, 50  
XML archive · 78

---