Manual

POLICY PATROL EMAIL

MAIL SECURITY



red earth
software

MANUAL

Policy Patrol Email

Mail Security

Version 10

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 © 2001-2014 by Red Earth Software. All rights reserved.

Contents at a Glance

1 Introduction 1

2 Pre-Installation 5

3 Installation 10

4 Importing Users 23

5 Email Threat Protection 33

6 Anti-Spam 41

7 Anti-Malware 79

8 Email Content Policies 87

9 Email Signatures 116

10 How to Order Policies 134

11 Creating Filters 137

12 Creating Templates 145

13 Quarantined Messages 172

14 Logs 196

15 Email Management 201

16 Mail Backup 206

17 Reporting 221

18 Settings 226

19 Dashboard 232

20 Server Administration 233

21 Troubleshooting 242

Table of Contents

1 Introduction 1

1.1 Why is Email Filtering Necessary? 1

1.2 Policy Patrol Email Editions 1

1.3 Policy Patrol Email Features 2

1.4 How Policy Patrol Addresses Email Threats 3

1.5 What's New in Version 10? 3

1.6 Why Policy Patrol? 4

1.7 Conventions 4

1.8 Manual Overview 4

2 Pre-Installation 5

2.1 System Requirements 5

2.2 Gathering Necessary Information 6

2.3 If You Have Exchange 2013/2010/2007 6

2.4 If You Have Exchange 2003 6

2.5 If You Have Lotus Domino 7

2.6 If You Have Another Mail Server 7

2.7 If You Have a Clustered Environment 7

2.8 If You Have a Frontend/Backend Server Setup 7

2.9 If You Wish to Share the Configuration Across Servers 8

2.10 If You Have Policy Patrol 7, 8 or 9 Installed 8

2.11 If You Have Policy Patrol 4, 5, or 6 Installed 8

2.12 If You Have Policy Patrol 1, 2 or 3 Installed 9

3 Installation 10

3.1 Installing Policy Patrol Server 10

3.2 Installing Policy Patrol Remote Administration Console 18

3.2.1 Connecting to the Policy Patrol Server 19

3.3 Policy Patrol Services 20

3.4 Modifying the Policy Patrol Installation 20

3.5 Uninstalling Policy Patrol 21

4 Importing Users 23

4.1 Licensing Users 23

4.2 Import from Active Directory 23

4.3 Import from Lotus Domino 25

4.4 Manually Import Users 26

4.4.1 Creating a Group Based on a Domain 27

4.4.2 Creating a Group Based on an LDAP Query 27

4.5 Using a Query filter to License Users 29

4.6 Editing Licensed Users 31

4.7 Auto-Licensing 31

4.8 Verify Users and Groups 32

5 Email Threat Protection 33

5.1 Configuring Email Threat Protection 33

5.2 Threat Classifications 33

5.2.1 Creating Threat Classifications 33

5.2.2 Editing Threat Classifications 37

5.2.3 Applying Threat Classifications 37

5.3 Anti-Spam 38

5.4 Anti-Phishing 39

5.5 Anti-Malware 39

5.6 Attachment Sanitization 39

6 Anti-Spam 41

6.1 Stop Spam Right Out of the Box 41

6.1 Allow Lists 41

6.1.1 Email Allow List 42

6.1.1.1 Email Allow List Exclusions 43

6.1.2 Word Allow List 44

6.1.3 IP Address Allow List 46

6.1.4 Configuring DNSWL Allow Lists 47

6.2 Block Lists 48

6.2.1 Email Block List 48

6.2.2 Word Block List 50

6.2.3 IP Address Block List 52

6.2.4 Countries Blocked 53

6.2.5 Character Set Blocking 53

6.2.6 DNSBL Lists 54

6.2.6.1 Change DNSBL Order 57

6.3 SURBL Lists 57

6.3.1.1 Change SURBL Order 58
6.4 Address Verification 58
6.4.1 Sender Verification 59
6.4.1.1 Sender Policy Framework (SPF) 59
6.4.1.2 DMARC Policies 59
6.4.1.3 Verify MX Record 60
6.4.1.4 Connect to Sender's SMTP Server . 60
6.4.1.5 Limit Delivery Status Notifications . 61
6.4.2 Email Harvesting 61
6.5 Greylisting 64
6.6 Bayesian Filtering 66
6.6.1 Importing Messages into the Bayesian Database 67
6.6.2 Editing Words in the Bayesian Database 68
6.7 Spam Characteristics 69
6.8 Options 71
6.8.1 Challenge/Response 71
6.8.1.1 Editing the Challenge/Response Email 72
6.8.2 Anti-Spam Exclusions 73
6.8.2.1 Internal IP Checking 73
6.8.2.2 Exclude Domains 73
6.8.2.3 DMZ 74
6.9 Forwarding Spam to the Users' Junk Mail Folders 74
6.9.1 If You Have Exchange 2007/2010/2013 74
6.9.2 Disabling Anti-spam 74
6.10 Changing the Order of Spam Checking Modules 74

7 Anti-Malware 79

7.1 Metascan Multi AV Scanner 79
7.2 Metascan Online and On-Premise 79
7.3 Metascan Online 80
7.4 Metascan On-Premise 81
7.5 Installing Metascan 81
7.6 Enabling Metascan in Policy Patrol 84
7.6.1 If Metascan is Installed on the Same Machine as Policy Patrol 84
7.6.2 If Metascan is Installed on a Separate Machine 85
7.7 Adding a Disclaimer 86
7.8 File Type Spoofing 86

8 Email Content Policies 87

8.1 Configuring an Email Content Policy 87
8.1.1 Step 1. Policy Users 88
8.1.2 Step 2. Policy Direction 88
8.1.3 Step 3. Policy Conditions 89
8.1.4 Step 4. Policy Exceptions 102
8.1.5 Step 5. Policy Actions 102
8.1.5.1 Primary Actions 102
8.1.5.2 Secondary Actions 103
8.1.5.3 Ordering of Secondary Actions 113
8.1.6 Step 6. Policy Scheduling 113
8.1.7 Step 7. Policy Name 114
8.2 Editing Existing Policies 114
8.3 Copying Policies 115
8.4 Moving Policies 115

9 Email Signatures 116

9.1 Configuring a Signature Policy 116
9.1.1 Step 1. Policy Users 117
9.1.2 Step 2. Policy Direction 118
9.1.3 Step 3. Policy Conditions 118
9.1.4 Step 4. Policy Exceptions 123
9.1.5 Step 5. Policy Actions 124
9.1.5.1 Primary Actions 124
9.1.5.2 Secondary Actions 124
9.1.5.3 Ordering of Secondary Actions 130
9.1.6 Step 6. Policy Scheduling 131
9.1.7 Step 7. Policy Name 131
9.2 Editing Existing Policies 132
9.3 Copying Policies 132
9.4 Moving Policies 132
9.5 Signature Position Maps 133
9.6 Viewing Signatures in Outlook Sent Items . 133

10 How to Order Policies 134

10.1 Ordering Policies 134
10.1.1 Processing Speed 134
10.1.2 Ordering Result 135
10.1.3 Process Next Policies 136

11 Creating Filters 137

11.1 Creating a Word/Phrase Filter 137

11.2 Creating an Attachment Filter 140
11.3 Creating an Email/Domain Filter 142
11.3.1 Active Directory Users in Email Filter . 143
11.4 Editing Filters 143
11.5 Copying Filters 144
11.6 Moving Filters 144
11.7 Content Checking Attachments 144

12 Creating Templates 145

12.1 Creating an Email Notification Template 145
12.2 Creating a Tag Template 148
12.3 Creating a Disclaimer/Signature Template 149
12.3.1 Creating a Standard Disclaimer/Signature Template 149
12.3.2 Creating an HTML Stationery Disclaimer Template 154
12.4 Inserting an Avatar in the Email Signature 159
12.5 Inserting a QR Code in the Email Signature161
12.6 Inserting Images or URLs from Active Directory 164
12.6.1 Inserting an AD Image into the Email Signature 164
12.6.2 Inserting a Personalized URL into the Email Signature 164
12.7 Editing Templates 165
12.8 Copying Templates 165
12.9 Moving Templates 165
12.10 Fields 165
12.10.1 User Fields 166
12.10.2 Message Fields 167
12.10.3 Date/Time Fields 168
12.10.4 Other Fields 168
12.11 Inserting AD Fields Depending on User's AD Information 169
12.11.1.1 Using a Prefix only if the Field Exists169
12.11.1.2 Avoiding an Empty Line if a Field Does Not Exist 169
12.11.1.3 Specifying a Default Value if a Field Does not Exist 170
12.12 Configuring Additional Directory Fields 170

13 Quarantined Messages 172

13.1 Creating Quarantine Folders 172
13.2 Editing Quarantine Folders 175
13.3 Quarantine Folder Permissions 176
13.4 Quarantine Folder Settings 177
13.5 Viewing Messages via the Administration Console 178
13.5.1 Message Report 178
13.5.2 Viewing Message Text and Headers 179
13.5.3 Email Threats Report 179
13.5.4 Email Content Policies Report 180
13.5.5 Email Signatures Report 180
13.5.6 Email Management Report 180
13.5.7 Viewing Details 180
13.5.8 Saving Down Attachments 181
13.5.9 Delivering Messages On Hold 181
13.5.10 Deleting Messages on Hold 182
13.5.11 Moving Messages on Hold 182
13.5.12 Multiple Messages 182
13.5.13 Folder Search 182
13.5.13.1 Simple Search 182
13.5.13.2 Advanced Search 183
13.5.14 Quarantine Reports 184
13.5.14.1 Configuring a User Quarantine Report 185
13.5.14.2 Configuring an Administrator Quarantine Report 187
13.5.14.3 Viewing the User Quarantine Report190
13.5.14.4 Viewing the Administrator Quarantine Report 191
13.6 Viewing Quarantine Folders via the Web Manager 192
13.6.1 Web Manager URL 193
13.6.2 Web Manager Permissions 193
13.6.2.1 Quarantined Items 194
13.6.2.2 Message History 194
13.6.2.3 Event History 194
13.6.2.4 Allow List 194
13.6.2.5 Block List 195

14 Logs 196

14.1 History 196
14.1.1 Message Report 197
14.1.2 Email Threats Report 197
14.1.3 Email Content Policies Report 198
14.1.4 Email Signatures Report 198
14.1.5 Email Management Report 198

14.1.6 Viewing Details 199
14.2 Event History 199
14.1 Audit Logs 200

15 Email Management 201

15.1 Auto Replies 201
15.2 POP3 Downloader 203

16 Mail Backup 206

16.1 Mail Backup 206
16.2 Enabling Mail Backup 206
16.3 Mail Backup Conditions 207
16.3.1 Selecting Users for Mail Backup 207
16.3.2 Specifying Mail backup Conditions 207
16.3.3 Specifying Mail Backup Exceptions 218
16.4 Message Retrieval 219

17 Reporting 221

17.1 Enabling Reporting 221
17.2 Running Reports 222
17.3 Auto Generating Reports 223
17.4 Available Reports 223
17.4.1 Spam Reports 223
17.4.2 Monitoring Reports 224
17.4.3 Anti-Virus Reports 224
17.4.4 Traffic reports 225
17.4.5 Policy Reports 225
17.4.6 Attachment Reports 225

18 Settings 226

18.1 Languages 226
18.2 Attachment Maps 227
18.3 Schedules 227
18.4 Web Manager Options 228
18.4.1 Allow List User Rights 229
18.4.2 Block List User Rights 230
18.4.3 Additional Options 231
18.5 Users 231

19 Dashboard 232

19.1 Email Threat Protection 232
19.2 Email Content Policies 232
19.3 Email Management 232
19.4 Email Signatures 232
19.5 Quarantine Folders 232

20 Server Administration 233

20.1 User Security 233
20.1.1 User Access Rights 233
20.1.2 Component Rights 234
20.1.3 Folder Rights 236
20.1.4 Inheritance of Folder Rights 237
20.2 Licensing 237
20.3 System Configuration 237
20.3.1 System Notifications 238
20.3.2 Exclude IP 238
20.3.3 Email Modifications 238
20.3.3.1 If You Have Multiple Exchange 2007/2010/2013 Servers 239
20.4 System Parameters 239
20.5 Automatic Update Settings 240
20.6 Import Policy Patrol Configuration 240
20.7 Export Policy Patrol Configuration 240
20.8 Disabling Policy Patrol 240
20.8.1 To Disable Policy Patrol 32-bit 240
20.8.2 To Disable Policy Patrol 64-bit 240
20.9 Enabling Policy Patrol 241
20.9.1 To Enable Policy Patrol 32-bit 241
20.9.2 To Enable Policy Patrol 64-bit 241

21 Troubleshooting 242

21.1 Knowledge Base 242
21.1.1 No Disclaimers are Being Added 242
21.1.2 My Sent Items in Outlook are not Being Updated 243
21.1.3 User Merge field is not Working 243
21.1.4 I Cannot Enter Licenses or Browse to Files or Folders 243
21.1.5 How Can I Copy the Configuration to Another Machine? 244
21.2 Send Support Files 244
21.3 Contacting Red Earth Software 244

Chapter 1

Introduction

Policy Patrol Email is a comprehensive email security solution that can block spam, phishing, confidentiality leaks, scripts, offensive content, viruses, manage disclaimers & signatures, compress and decompress attachments, archive emails and more.

1.1 Why is Email Filtering Necessary?

Email is a great business tool. It's fast, cheap, universal and easy to deploy. However, companies that make use of email are confronted with a number of risks:

- Legal liability
- Damage to reputation
- Loss of productivity
- Network congestion
- Confidentiality breaches
- Regulatory compliance

1.2 Policy Patrol Email Editions

In combination with a sound email policy, Policy Patrol helps companies protect themselves against these threats and gain more control over their email system. In addition, Policy Patrol can be a valuable marketing tool by allowing your company to add consistently branded email signatures along with banners promoting the latest events and promotions. Policy Patrol is available in the following editions:

Policy Patrol Disclaimers (email disclaimers & signature management)

Policy Patrol Mail Security (anti-spam & anti-phishing, anti-malware, email content policies, email backup, disclaimers/signatures)

Policy Patrol Mail Security includes all features included in Policy Patrol Disclaimers. If you purchased Policy Patrol Disclaimers, it is always possible to upgrade to the Policy Patrol Mail Security at a later stage in order to gain access to additional features. If you are interested in this, please send an email to sales@redearthsoftware.com and we can provide you with a 30-day evaluation version. You will not need to reinstall the program and your existing configuration will remain intact. After the evaluation period, you can return to the Policy Patrol Disclaimers version by entering your previous serial number. Your configuration will be intact.

1.3 Policy Patrol Email Features

The table below shows a list of the features included in each Policy Patrol edition:

Feature	Policy Patrol Disclaimers	Policy Patrol Mail Security
User and condition based mail backup		✓
Message search and retrieval		✓
Compression and decompression of attachments		✓
Advanced disclaimers & signatures	✓	✓
Send blind copy	✓	✓
Email branding/HTML stationery	✓	✓
Advanced blocking of spam & phishing emails		✓
Monitor messages via web browser		✓
Users monitor their own spam messages		✓
Daily quarantine reports via email		✓
Block & Allow lists		✓
Spam reports		✓
Move messages to folder		✓
Intelligent keyword filtering		✓
Delay messages		✓
Reports on email usage and statistics		✓
Email and network notifications		✓
Attachment checking		✓
Virus scanning		✓**
Customize NDRs and DSNs		✓
Convert HTML into plain text		✓
Auto print emails (to printer or pdf)		✓
Add X-header		✓
Run program		✓
Change message priority		✓
Add business card (vCard)	✓	✓
Add/remove attachment		✓
Automatically add sender or recipient to filter		✓
Automatically remove sender or recipient from filter		✓
Auto replies	✓	✓
Remove read/delivery receipt requests		✓

Flexible user and group based rules	✓	✓
Advanced user permissions	✓	✓

* Only inbound messages
**Additional module

1.4 How Policy Patrol Addresses Email Threats

Each Policy Patrol edition addresses different email threats. Policy Patrol Disclaimers decreases the threat of legal liability, damage to reputation and confidentiality breaches and can also help ensure regulatory compliance and consistent company email branding. Policy Patrol Mail Security offers a complete solution by addressing all email risks; by blocking spam, Policy Patrol Mail Security reduces network traffic and improves employee productivity. in addition to adding disclaimers and signatures and blocking spam, this product ensures regulatory compliance, reduces legal liability and prevents damage to reputation & confidentiality breaches by content checking emails and their attachments. In addition, by backing up emails and compressing attachments, Policy Patrol Mail Security reduces network congestion, storage requirements and lost productivity.

Email threat	Policy Patrol Disclaimers	Policy Patrol Mail Security
Lost productivity		✓
Network congestion		✓
Increased storage space needs		✓
Legal liability	✓	✓
Damage to reputation	✓	✓
Confidentiality breaches		✓
Regulatory compliancy	✓	✓
Inconsistent company email branding	✓	✓

1.5 What's New in Version 10?

Policy Patrol 10 offers increased protection from email security risks, as well as an improved user interface and new dashboard.

New features in version 10:

- New Real-Time Phishing Block List
- Improved Handling of Spoofed Emails with DMARC
- Metascan Online Multi Anti-Virus Scanning (free edition*)
- New Dashboard with Instant Overview of Threats Detected
- Audit Logs Now Accessible From Console
- New Test Email Feature for Email Signatures
- Improved User Interface
- Policy Patrol Mail Security 10 users free!

* A free Metascan Online subscription is included for scanning up to the free edition scan limits. Licenses for increased scan limits are available for purchase.

1.6 Why Policy Patrol?

Policy Patrol distinguishes itself from other email filtering products by offering companies unmatched flexibility in configuring policies based on users, conditions, exceptions and actions. Policy Patrol is a scalable solution that can grow with your business, allowing you to add more users or features at a later stage without having to install new software. Policy Patrol Email includes many unique email management features not found in other products and is always the first to add exciting new features; Policy Patrol was the first to use Active Directory merge fields in the email signature and show the email signature in Outlook Sent Items. Policy Patrol was the first commercial anti-spam product to use SURBL lists for spam blocking, something which is now standard in most anti-spam solutions.

1.7 Conventions

Conventions used in this manual:

- **Bold text** is used to signify a selection or button, for instance the **Deliver** button, or the option **Move to Folder**.
- `Courier font` is used to signify text that must be entered in the program, for instance enter `bloggs.com` and click **Submit** to add the domain to the allow list.
- Paragraph and chapter names are listed in between parentheses, for instance for instructions on how to install Policy Patrol, consult chapter 3 'Installation'.
- Keys are displayed in capitals and in between brackets, such as [CAPS], [TAB] or [DELETE].
- Throughout the manual there are Tips, Info and Notes that contain useful information:

Note type:	Contains:
Tip	Useful information to get the best out of Policy Patrol
Info	More in-depth, background information
Note	Important notes that you should be aware of

-

1.8 Manual Overview

Chapters 2-4 guide you through the general installation & set up of Policy Patrol. Other chapters focus on particular parts of the program. According to the functionality that you will be using you can pick and choose which chapters you wish to read through.

Chapter

2

Pre-Installation

This chapter describes the system requirements for Policy Patrol and includes instructions for deploying Policy Patrol with different mail servers and different mail server set ups.

2.1 System Requirements

Policy Patrol requires the following to be installed:

Policy Patrol Email (64-bit version):

- ☑ Windows Server 2003, 2008/2008 R2, 2012/2012 R2.
- ☑ Microsoft Exchange Server 2013, 2010, Exchange 2007 or Windows Small Business Server 2008/2011.
- ☑ Microsoft .NET Framework 2.0 (If you do not have this installed the Policy Patrol installation program will install it for you)

Policy Patrol Email (32-bit version):

- ☑ Windows Server 2003
- ☑ Microsoft Exchange Server 2003, Windows Small Business Server 2003, or Lotus Domino R5-R8 or other mail server.
- ☑ Microsoft .NET Framework 2.0 (If you do not have this installed the Policy Patrol installation program will install it for you)

Note

Microsoft Outlook must not be installed on the same machine as Policy Patrol (except for remote administration).

2.2 Gathering Necessary Information

Before proceeding to install and configure Policy Patrol, make sure you have the following information:

☑ Name or IP address of your mail server

☑ Check whether any of the following paragraphs apply and follow the appropriate instructions.

2.3 If You Have Exchange 2013/2010/2007

Policy Patrol (64-bit) can be installed on an Exchange 2013, 2010 or 2007 machine using any of the following roles:

☑ Hub Transport Role

☑ Edge Transport Role (requires access to Active Directory)

For instructions on how to install Policy Patrol on a separate machine without Exchange Server, download the following document (remember that if you install Policy Patrol on a non-Exchange Server machine, Policy Patrol will not process internal mails, and Outlook sent items will not be updated):

Installing Policy Patrol on a separate machine

(http://www.policypatrol.com/assets/pp10-separatemachine.pdf)

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

2.4 If You Have Exchange 2003

If you have Exchange 2003 you can install Policy Patrol on the Exchange Server machine (recommended) or on a separate machine. If you are installing Policy Patrol on the same machine as Exchange Server, proceed to chapter 3 'Installation'.

For instructions on how to install Policy Patrol on a separate machine without Exchange Server, download the following document (remember that if you install Policy Patrol on a non-Exchange Server machine, Policy Patrol will not process internal mails, and Outlook sent items will not be updated):

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

2.5 If You Have Lotus Domino

If you are using Lotus Domino R5-8 you must install Policy Patrol on a separate Windows 2003/2008/2012/XP machine. Policy Patrol does not offer internal mail filtering for Lotus Domino. Policy Patrol can retrieve Lotus Domino users & groups, and their user properties for the user fields. Download the following document for instructions on how to install Policy Patrol with Lotus Domino:

Installing Policy Patrol with Lotus Domino
(http://www.policypatrol.com/assets/pp10-lotusdomino.pdf)

2.6 If You Have Another Mail Server

If you are using another mail server than Exchange Server or Lotus Domino, you must install Policy Patrol on a separate Windows 2003/2008/2012 machine. If you have Active Directory installed, Policy Patrol will be able to retrieve your users, groups, and merge fields from the Active Directory. If you do not have Active Directory installed, you can manually input or import your users and email addresses in Policy Patrol.

2.7 If You Have a Clustered Environment

Policy Patrol (32-bit and 64-bit) can be installed in a clustered environment. However if you have Exchange Server 2003, Policy Patrol can only be installed in Active/Passive clusters, not Active/Active clusters. To install Policy Patrol in an Exchange 2003 clustered environment, download the document below for further instructions:

Installing Policy Patrol in a 32-bit cluster
(http://www.policypatrol.com/assets/pp10-clustering.pdf)

If you are installing Policy Patrol 64-bit in a cluster, there are no specific cluster instructions to follow; you can simply follow the instructions for a regular installation in paragraph 3.

Note: You need to purchase an additional server license for the clustered node. The additional server license cost is found in the price list at http://www.policypatrol.com/pricing. For more information, please send an email to sales@redearthsoftware.com.

2.8 If You Have a Frontend/Backend Server Setup

Policy Patrol must always be installed on the backend server. However if you use email clients that are using the frontend server to relay their email, you must install Policy Patrol on the frontend server as well as the backend server.

Note: You need to purchase an additional server license for each additional Policy Patrol server installation. The additional server license cost is found in the price list at http://www.policypatrol.com/pricing. For more information, please send an email to sales@redearthsoftware.com.

2.9 If You Wish to Share the Configuration Across Servers

Policy Patrol allows you to share a configuration across multiple servers by separating the Policy Patrol Server that holds the configuration and processes the messages, from the Policy Patrol Agents that capture and deliver the messages. Policy Patrol Agents can be installed on different machines than the Policy Patrol Server. Requests captured by the agents will be processed on the Policy Patrol Server and returned to the Agent for delivery.

The Policy Patrol Server can be installed on a machine with Exchange Server installed or without. If it's installed on an Exchange Server machine there is no need to install the Policy Patrol Agent on that machine (since it is included with the installation). You will then only need to install the Policy Patrol Agents on the Exchange Servers where Policy Patrol Server is not installed. If you install the Policy Patrol Server on a machine without Exchange installed, you need to install the Policy Patrol Agents on all Exchange Servers on which you would like to process messages. For Exchange 2007/2010/2013, Policy Patrol Agents need to be installed on the Exchange Servers with the Hub or Edge Transport role.

For more information on how to deploy Policy Patrol Servers and Policy Patrol Agents in order to share a configuration:

Sharing a Policy Patrol Configuration
(http://www.policypatrol.com/assets/pp10-sharedconfiguration.pdf)

Note: You need to purchase an additional server license for each additional Policy Patrol Agent (i.e. one Policy Patrol Agent is included in your initial license, but you must purchase an additional server license for any additional Policy Patrol agents that are installed). The additional server license cost is found in the price list at http://www.policypatrol.com/pricing. For more information, please send an email to sales@redearthsoftware.com.

2.10 If You Have Policy Patrol 7, 8 or 9 Installed

To upgrade from version 7, 8 or 9 to version 10, simply start the Policy Patrol 10 installation and you will automatically be upgraded to version 10 (all your configuration settings will be kept). For more information on how to upgrade to version 10, download the following document:

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

2.11 If You Have Policy Patrol 4, 5, or 6 Installed

To upgrade from version 4, 5 or 6 to version 10, you must first upgrade to version 7 and then upgrade to version 10 following the instructions above. For more information on how to upgrade to version 7, download the following document:

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

2.12 If You Have Policy Patrol 1, 2 or 3 Installed

Before you install version 10, you must uninstall Policy Patrol by going to Add/Remove programs. Since there have been many updates to the program, it is not possible to use your configuration files in version 10.

Chapter

3

Installation

This chapter describes the steps for installing Policy Patrol. It also discusses how to set up remote administration and the different services that the program installs.

3.1 Installing Policy Patrol Server

Note

Note that if you are installing Policy Patrol on a separate machine without Exchange Server, you must consult the appropriate sections in the chapter 'Pre-installation'.

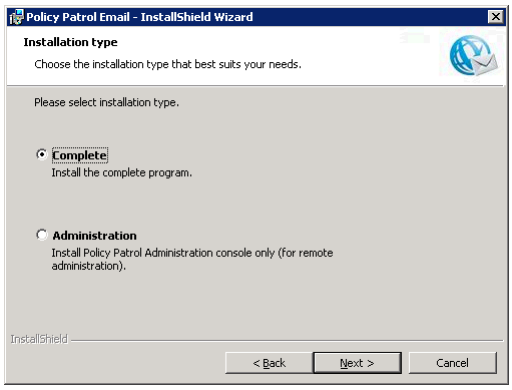
To install Policy Patrol follow the next steps:

1. Double-click on **PolicyPatrol.exe** (32-bit version) or **PolicyPatrol64.exe** (64-bit version). The Install Program will start up. If you do not have Microsoft .NET Framework installed, the Policy Patrol installation program will install it for you.

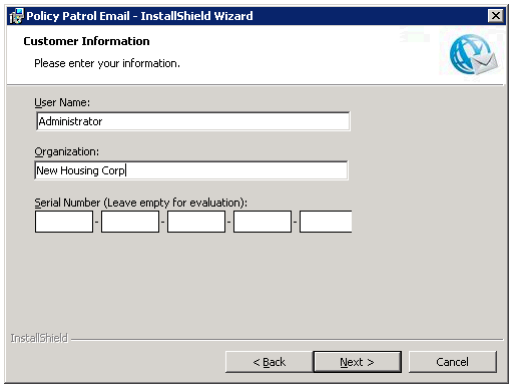
2. In the Welcome screen, click **Next**.

3. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.

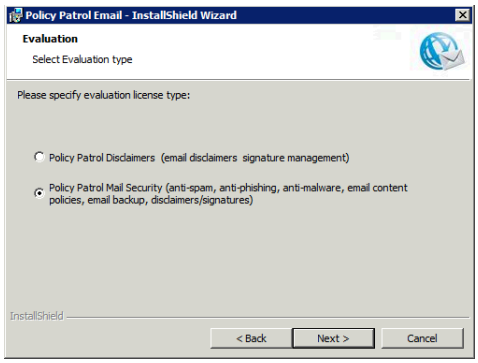
4. Select the installation type. If you select **Complete**, the complete program will be installed. If you only wish to install the Administration console (for remote administration), select **Administration**.



5. Enter your user name, company name and Policy Patrol serial number. If you are evaluating Policy Patrol, leave the serial number field empty. Click **Next**.



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

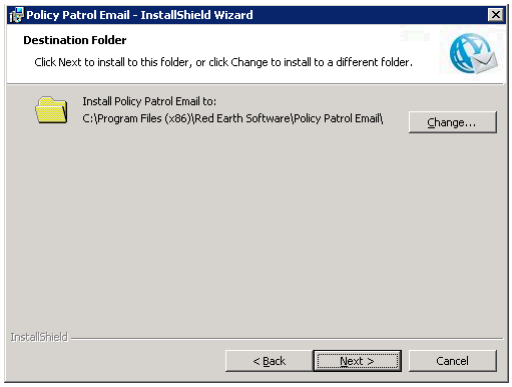


Tip

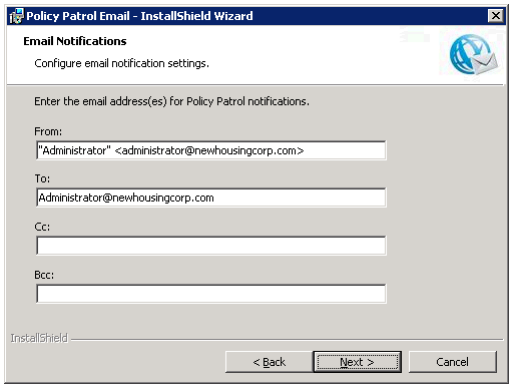
If you are evaluating Policy Patrol and later wish to try out a different Policy Patrol edition follow the next steps: After installation, open the Policy Patrol Administration console and go to **<server name>** > **Security** > **Licenses**, select the license and click **Remove**. Policy

Patrol will warn that no valid license is found. Click **OK**. A dialog will now pop up allowing you to select a new evaluation license type.

7. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email (32-bit version) or C:\Program Files (x86)\Red Earth Software\Policy Patrol Email (64-bit version). If you wish to change the location, click **Change** and select another folder. When you are ready, click **Next**.

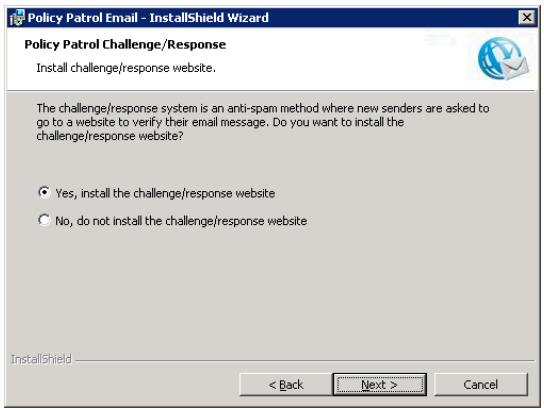


8. Specify the email notification settings. Enter the From:, To:, Cc: and Bcc: fields for the Policy Patrol notification emails. Policy Patrol notification emails inform you about evaluation expiry dates, licensing issues and new updates to the program. The From: display name is pre-configured as Administrator, but you can change this by entering the following: "Display name" <email address>, i.e. "Joe Bloggs" <jbloggs@bloggsco.com>. Click **Next**.

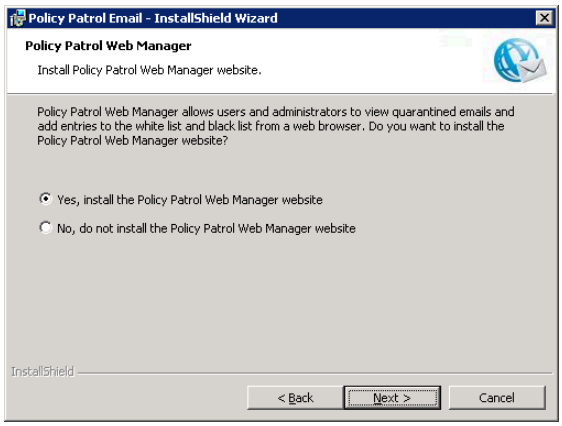


9. Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected **No, disable spam filtering**, continue to step 12.

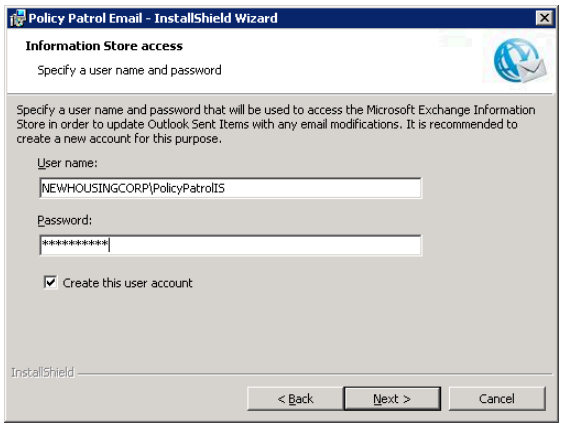
10. **If you selected to enable spam filtering**: Select whether you wish to install the challenge/response website. This website is needed if you wish to make use of the challenge/response system that asks new senders to go to a website and verify their email in order for the message to be delivered. Click **Next**.



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



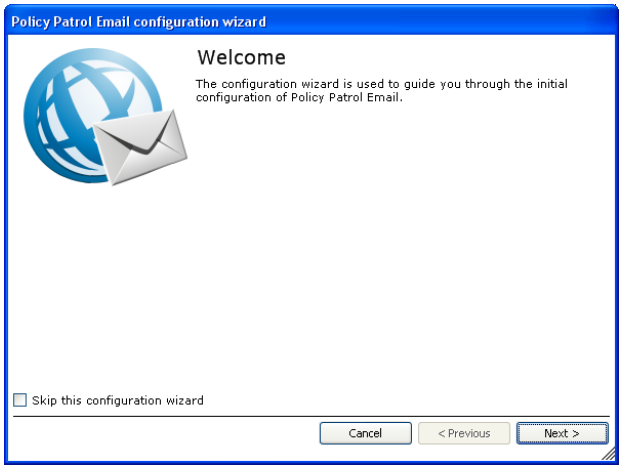
12. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please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



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

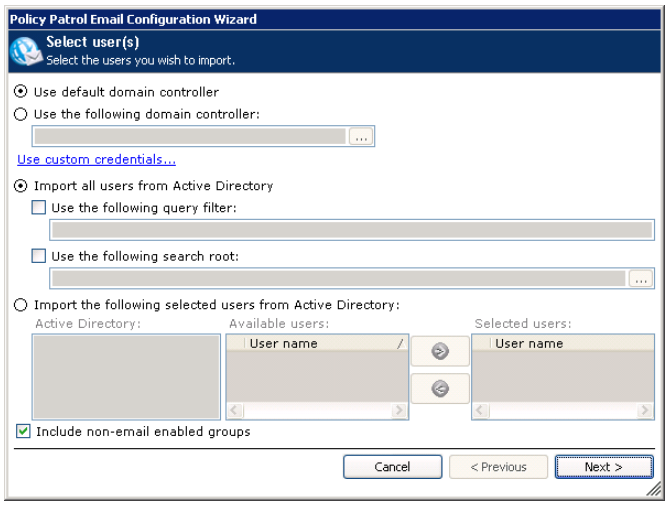
14. When the installation wizard has finished copying the files, click **Finish**.

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

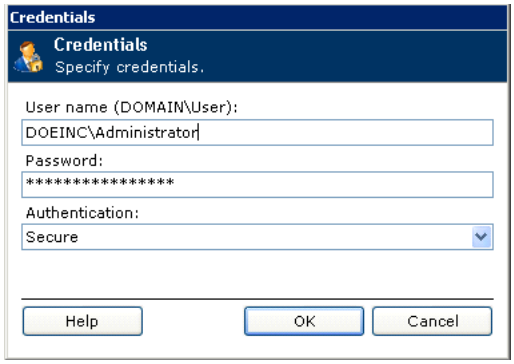


16. Specify the location from where you would like to import your users (Active Directory, Lotus Domino or Manual input). For more detailed information, consult chapter 4. Click **Next**. (Note: the 64-bit version only includes the Active Directory and Manual Input options.)

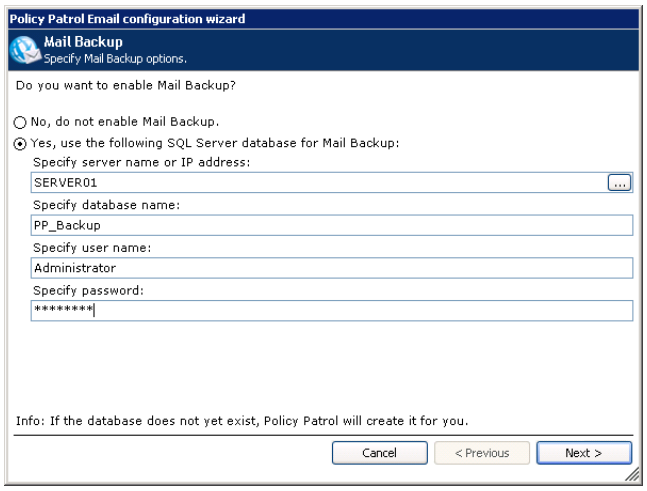
17. Specify the server or domain controller and select the users that you wish to license. You can either license all users or you can select only certain users to be licensed. For more information on the different options, consult chapter 4. Click **Next**.



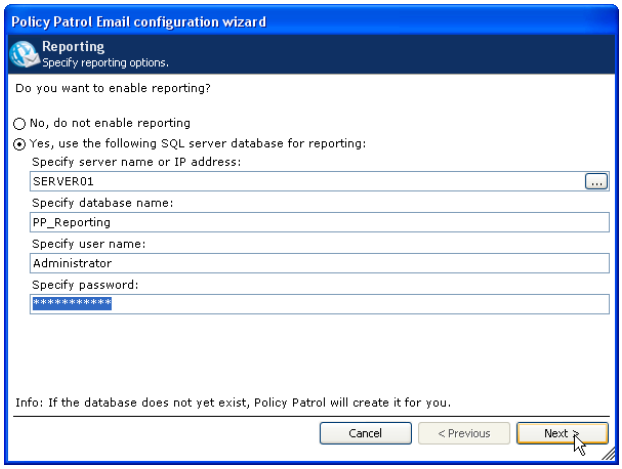
If you need to use a different user account than the account you are logged on with in order to retrieve users (for instance, this can be the case if you need to retrieve users from a different Active Directory sub domain), click on **Use custom credentials**. A dialogue will appear where you can enter your user name (DOMAIN\User), e.g. `DOEINC\Administrator`, the password and the authentication method. A number of authentication options are available, including Secure, Encryption, Anonymous, Secure Sockets Layer, etc. If you are not sure which Authentication option to choose, select **None**.



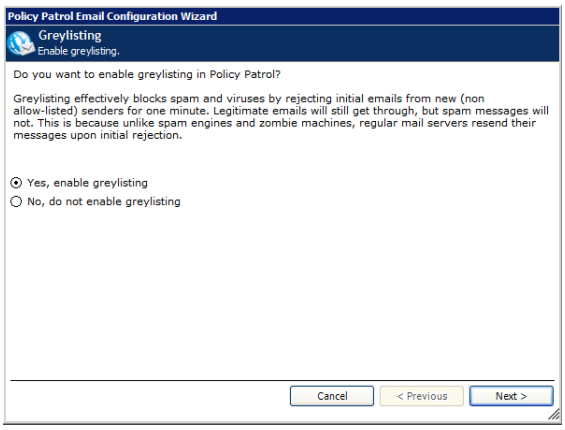
18. Select whether you wish to enable Mail Backup. If you enable Mail Backup you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically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



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

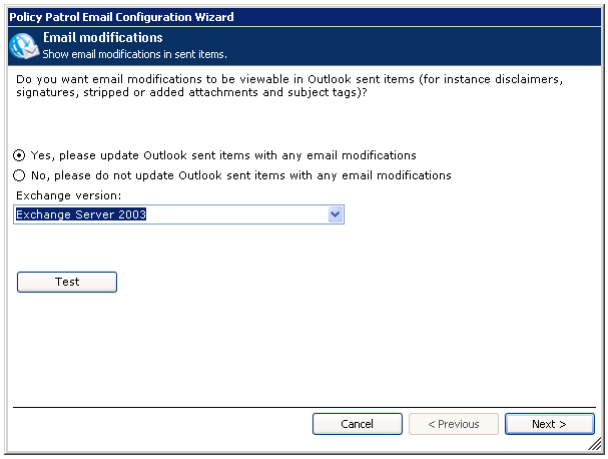


20. Select whether you wish to enable greylisting. Greylisting effectively blocks spam and viruses by initially rejecting messages from new, non white-listed senders for one minute, therefore allowing legitimate emails through without any user intervention, and blocking the non-legitimate emails. Select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

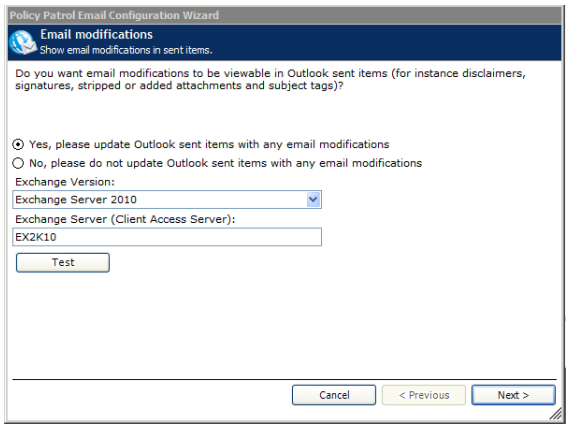


21. Select whether you wish to view email modifications in Outlook Sent items. If you select **Yes**, any modifications that are applied to outgoing emails by Policy Patrol, such as disclaimers, signatures, subject tags and adding or stripping attachments, will automatically show in Outlook Sent Items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

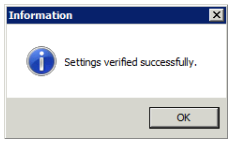
    If you have Exchange 2003: In 'Exchange version', Exchange Server 2003 should be selected.



    If you have Exchange 2007/2010/2013: In 'Exchange version', your Exchange version should be selected (Exchange Server 2007, Exchange Server 2010 or Exchange Server 2013). In 'Exchange Server (Client Access Server)' the name of your Exchange Client Access Server should be listed (even if this is the same machine as Policy Patrol is installed on). If you only have one Exchange Server, the name of the local server should be listed. If you have multiple Exchange Servers, you need to enter the name of your Client Access Server (CAS). If you have multiple Client Access Servers (load balancing) you need to enter the virtual IP address that is used for load balancing. The Policy Patrol Sent Items updates will then also be load balanced.



To check whether the settings are correct, click **Test**. Select a user from the list. Policy Patrol will verify whether the mailbox can be accessed. If successful, the message 'Settings verified successfully' will be shown.



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

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

IMPORTANT: Please exclude the Policy Patrol directory (C:\Program Files\Red Earth Software\Policy Patrol Email (32-bit version) or C:\Program Files (x86)\Red Earth Software\Policy Patrol Email (64-bit version)) from any anti-virus file scanning software and automated backup software since this could cause Policy Patrol not to function correctly due to inability to access files whilst these programs are scanning the Policy Patrol directory.

3.2 Installing Policy Patrol Remote Administration Console

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 Server 2012/2012 R2, 2008/2008 R2 or 2003, Windows XP Professional or Windows 7/8.
- ☑ Microsoft .NET Framework 2.0. If you do not have this installed the Policy Patrol program will download and install it for you.

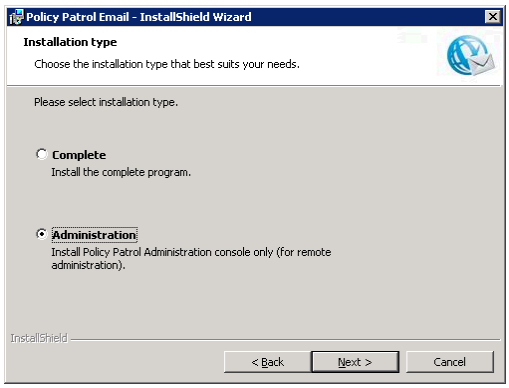
To install the Policy Patrol Remote Administration Console:

1. Double-click on **PolicyPatrol.exe** (32-bit version) or **PolicyPatrol64.exe** (64-bit version). The Install Program will start up. If you do not have Microsoft .NET Framework installed, the Policy Patrol installation program will download it for you.

2. In the Welcome screen, click **Next**.

3. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.

4. Select **Administration** as the installation type.



5. Enter your user name and company name. Click **Next**.

6. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email (32-bit version) or C:\Program Files(x86)\Red Earth Software\Policy Patrol Email (64-bit version). If you wish to change the location, click **Change** and select another folder. When you are ready, click **Next**.

7. Click **Install** to start installing.

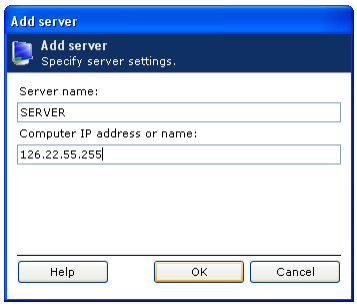
8. When the installation wizard has finished copying the files, click **Finish**.

3.2.1 Connecting to the Policy Patrol Server

After installing the Administration console for remote administration you must enter the details of the Policy Patrol server and connect to it. To do this, follow the next steps:

1. Click on **Add server**.

2. Enter the installation name and the computer name or IP address of the Policy Patrol installation. Click **OK**.



3. Select the newly added installation and click **Connect**. If you wish to automatically connect to this installation when opening the Administration console, select the option **Auto connect to this server when opening Policy Patrol Administration**.

Note

When managing Policy Patrol remotely, you will have to enter the path to folders (instead of browsing) and you will not be able to access Licensing to enter or change serial numbers. Furthermore, if you have Microsoft Outlook installed on the remote machine, you will not be able to view the body of internally sent messages in Monitoring. This is because internal messages are in a proprietary format (TNEF), which cannot be decoded when Outlook is installed on the same machine.

3.3 Policy Patrol Services

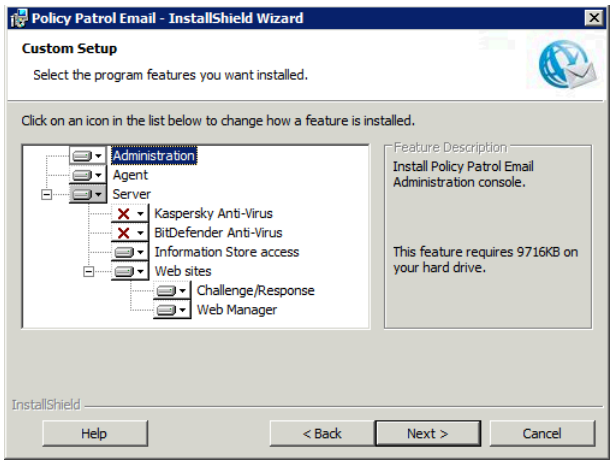
Policy Patrol installs a number of services on the machine. The following services are installed:

- ✓ Policy Patrol Email Server Service (if this service is stopped you will no longer be able to access your configuration)
- ✓ Policy Patrol Email Simple Information Store Access - (if this service is stopped you will no longer see email modifications in Outlook Sent Items)

3.4 Modifying the Policy Patrol Installation

If you wish to add or remove components from the Policy Patrol installation at a later stage, you can do so as follows:

1. Go to **Start** > **Settings** > **Control Panel** > **Programs and Features**.
2. Select **Policy Patrol Email** and click **Change/Remove**.
3. The installation wizard will start up. Select **Modify** and click **Next**.



4. You will now be able to select the program components that you wish to remove or add. Make sure that for the features that you wish to install, the option 'This feature will be installed on local hard drive' is selected from the drop-down list. For all components that you do not wish to install or wish to remove, you should select 'This feature will not be available' from the drop-down list. Note that the Administration console cannot be removed. You can choose to install or de-install the following components:

   - **Agent** – Policy Patrol Agent (intercepts messages).
   - **Server** – Policy Patrol Server (processes messages).
   - **Information Store access** – Install this component to allow Policy Patrol access to the Exchange Information Store to update Outlook Sent Items with any email modifications.
   - **Web sites > Challenge/Response** - Policy Patrol Challenge/Response web site (only for Policy Patrol Spam Filter and Policy Patrol Mail Security)
   - **Web sites > Web Manager** - Policy Patrol Web Manager web site (only for Policy Patrol Spam Filter and Policy Patrol Mail Security)

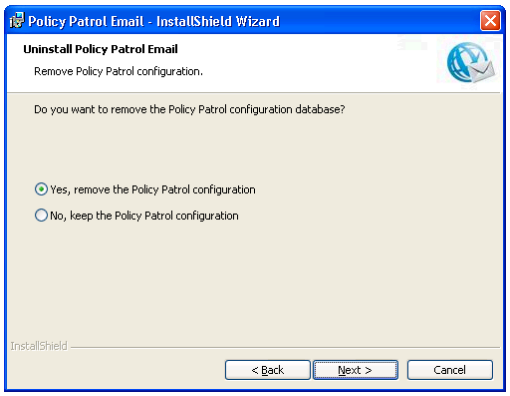
   When you have made your selections, click **Next**

5. The installation program will now copy or remove the necessary files. Click **Finish** to complete the operation.

3.5 Uninstalling Policy Patrol

To uninstall Policy Patrol, follow the next steps:

1. Go to **Start** > **Settings** > **Control Panel** > **Programs and Features.**
2. Select Policy Patrol Email in the list and click on the **Change/Remove** button.
3. Select **Remove** and click **Next**.



4. Select whether you wish to remove the Policy Patrol configuration. Important: If you select **Yes, remove the Policy Patrol configuration** you will no longer be able to retrieve your existing Policy Patrol settings. Click **Next**.

5. The program will start removing the installation. When the Maintenance complete dialog pops up, click **Finish**.

Chapter

4

Importing Users

This chapter describes how to import users and groups into Policy Patrol using Active Directory, Lotus Domino or manual input. It also discusses how to create groups per domain, how to make use of LDAP queries and how to auto license users.

4.1 Licensing Users

Policy Patrol user licensing is extremely flexible in that it allows you to only license the users that you wish to create rules for. You must select licensed users by importing users from Active Directory, Lotus Domino or by entering them manually. To add licensed users follow the instructions below for the appropriate import source.

> **Note**
>
> Each mailbox is counted as a user license. This means that only primary SMTP addresses are counted, not proxy addresses. Groups without email addresses are not counted as users, but groups with an email address (e.g. sales@company.com) are counted as users.

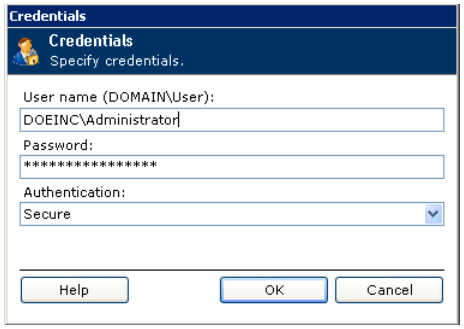
4.2 Import from Active Directory

If you have Exchange 2013, 2010, 2007 or 2003 and/or Active Directory, you must retrieve your users from the Active Directory by following the next steps:

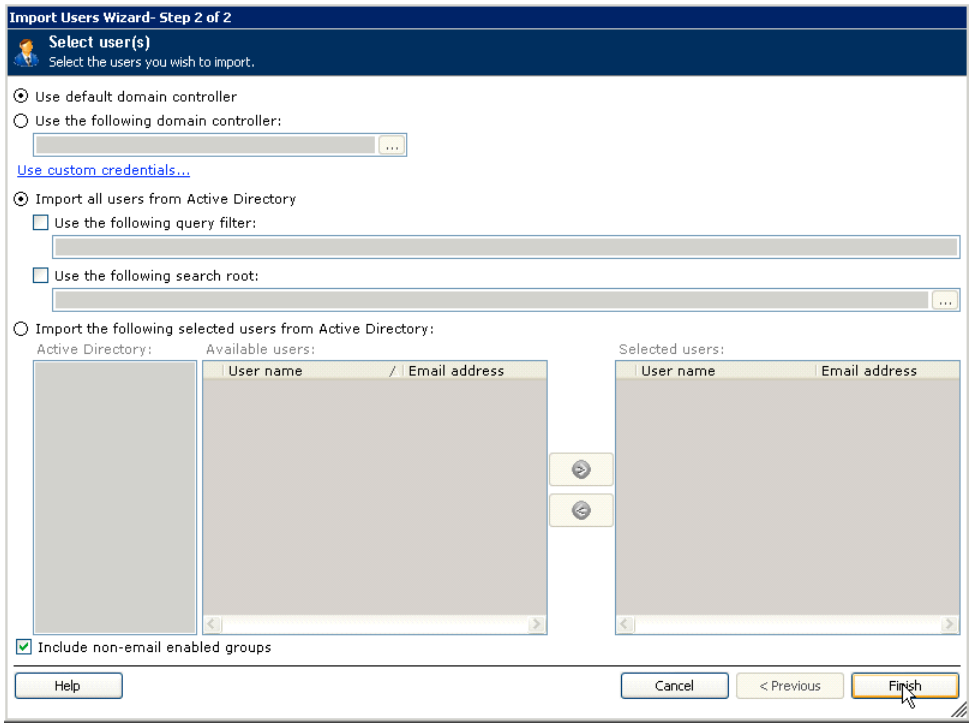
1. Go to **Settings** > **Users** and click on **Add...**.
2. In the Welcome screen, click **Next**.
3. Select **Active Directory** and click **Next**.
4. Leave the option **Use default domain controller** selected, or if you wish to retrieve users from another domain controller, select **Use the following domain controller**. Click **...**, select the domain controller you wish to retrieve your users from and click **OK**.

   If you need to use a different user account than the account you are logged on with in order to retrieve users (for instance, this can be the case if you need to retrieve users from a different Active Directory sub domain), click on **Use custom credentials**. A dialogue will

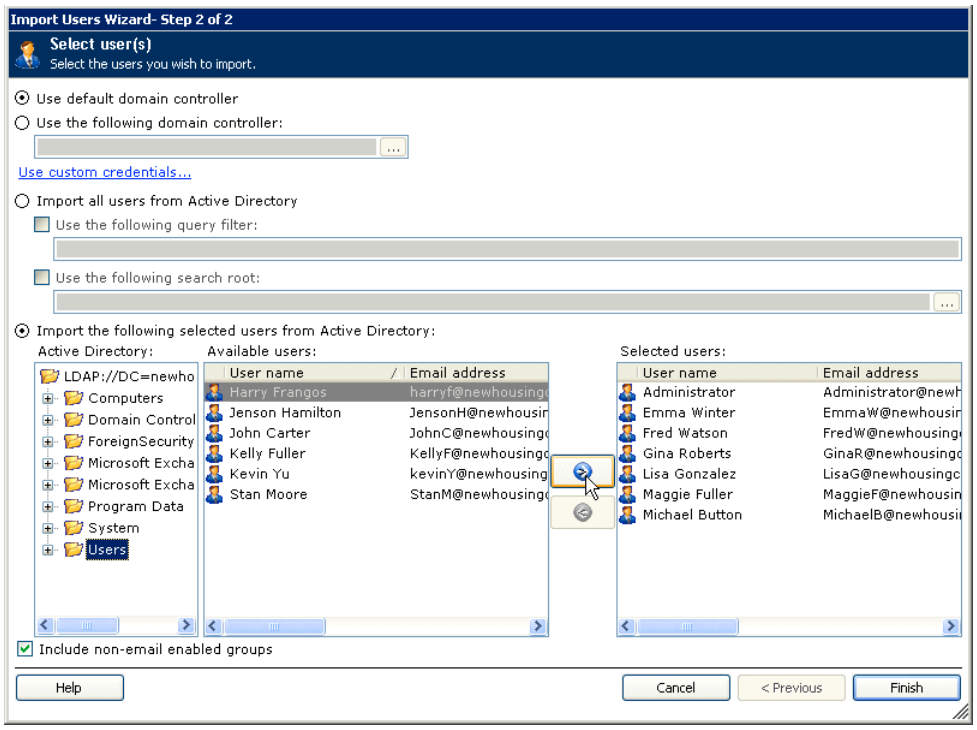
appear where you can enter your user name (DOMAIN\User), e.g. `DOEINC\Administrator`, the password and the authentication method. A number of authentication options are available, including Secure, Encryption, Anonymous, Secure Sockets Layer, etc. If you are not sure which Authentication option to choose, select **None**.



To import all users from the Active Directory, select the option **Import all users from Active Directory**. You can also enter a custom query filter to import all users with a certain attribute. To do this, select **Use the following query filter** and enter your query. For more information on creating a query filter, see the paragraph 4.5 'Using a query filter to license users'. If you only want to import users from a certain search root, select the option **Use the following search root** and enter the Active Directory search root where you would like to retrieve your users from.



To import selected users from Active Directory, select the option **Import the following selected users from Active Directory**. Browse to the root in the Active Directory where you wish to import your users from. Select the users you wish to license in the left pane and press ➔. The selected users will now appear in the right pane. To remove users, press the ➔ button.



If you wish to create policies based on Active Directory Groups, you must check the option **Include non-email enabled groups**. This will for instance allow you to select the sales group when configuring a policy, so that Policy Patrol will automatically apply the policy to all members of the sales group. If you don't tick this check box, Policy Patrol will only retrieve and license email enabled groups. For instance if the sales group uses the email address sales@company.com, this group will automatically be licensed. If you specified to only license selected users, Policy Patrol will only include non-email enabled groups that the selected users are members of. When you are ready, click **Next**.

Note

An email-enabled group is counted as one license. For non-email-enabled groups, Policy Patrol only licenses the members, not the groups themselves.

When you are ready, click **Finish**. You will now see your users in the Licensed user list **Settings** > **Users**.

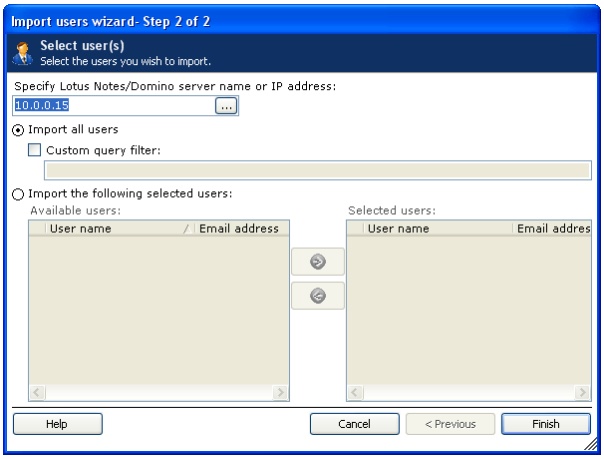
4.3 Import from Lotus Domino

If you have Lotus Domino without Active Directory, you must retrieve users from Lotus Domino by following the next steps (this option is only available in the 32-bit version):

1. Go to **Settings** > **Users** and click on **Add...**.
2. In the Welcome screen, click **Next**.

3. Select **Lotus Notes/Domino** and click **Next**.

4. Enter your Lotus Domino server name or IP address, or click **...** to browse to the computer. If your LDAP service is listening on a different port than 389, you must also enter the LDAP port as follows: `<IP address>:<LDAP port>`, e.g. `10.0.0.15:390`.



To license all users in Lotus Domino, select **Import all users**. You can also enter a custom query filter to import all users with a certain attribute. For more information, see the paragraph 'Custom query filter'. If you only wish to license certain users, select **Import the following selected users**. Select the users you wish to license in the left pane and press ➔. The selected users will now appear in the right pane. To remove users, press the ➔ button. When you are ready, click **Finish**. You will now see your users in the Licensed user list in **Settings** > **Users**.

4.4 Manually Import Users

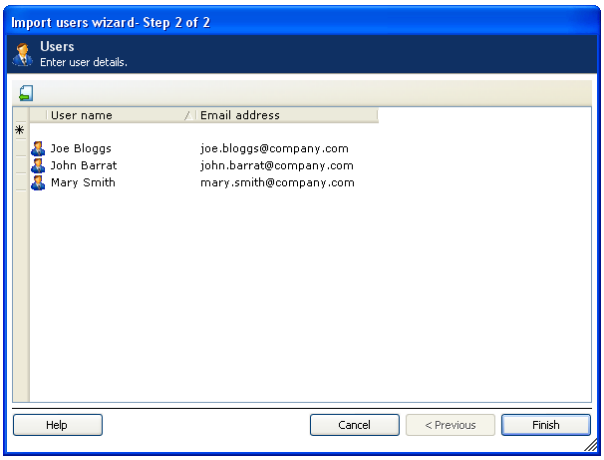
If you have another mail server without Active Directory, you must manually input your users by following the next steps:

1. Go to **Settings** > **Users** and click on **Add...**.

2. In the Welcome screen, click **Next**.

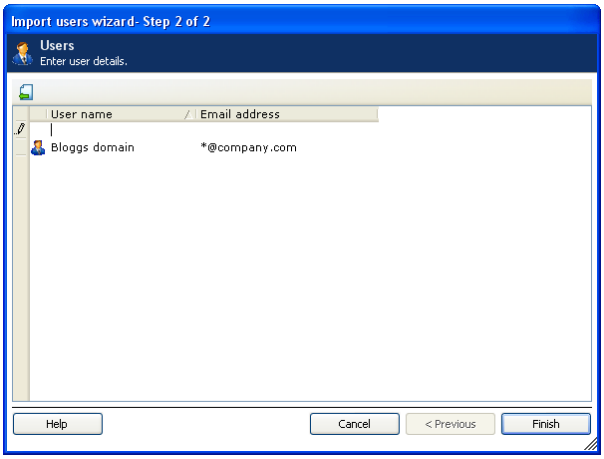
3. Select **Manual input** and click **Next**.

4. Enter the user names and email addresses. If you wish to import users from a text file you can click on the **Import** button in the toolbar. The data in the text file must be entered as follows: `First Name Last Name;email address`. For instance: `Mary Smith;mary.smith@company.com`. Instead of a semi colon (;) you can also use a comma (,) or a [TAB] as a separator. Each user must be listed on a separate line. When you are ready click **Finish**. You will now see your users in the Licensed user list in **Settings** > **Users**.



4.4.1 Creating a Group Based on a Domain

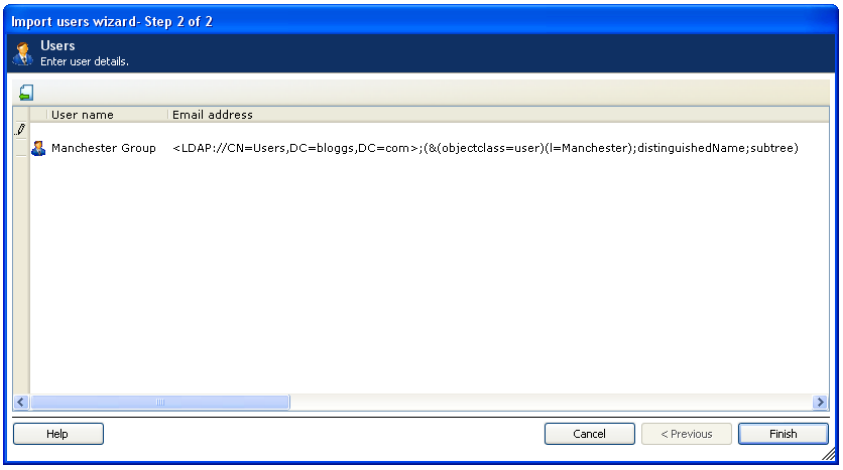
If you want to apply policies based on domain, you can configure a group that includes all users of a certain domain. To do this you must go to **Settings** > **Users**. Click on **Add**. Click **Next** in the Welcome screen, select **Manual input** and click **Next**. Now enter the group name in the 'User name' field, for instance `Bloggs domain`. In the 'Email address' field enter the domain preceded by a * and @, i.e. `*@bloggs.com`. Click **Finish**. When configuring policies, you will now be able to select the user 'Bloggs domain' which will include all licensed users whose email addresses end in the domain entered, for example bloggs.com. Remember however that you still need to license the users in Policy Patrol by importing them from Active Directory, Lotus Domino or by making use of manual input.



4.4.2 Creating a Group Based on an LDAP Query

If you want to apply policies to users that have certain Active Directory attributes, you can configure a custom group that uses an LDAP search query. To do this, you must go to **Settings** > **Users**. Click on **Add**. Click **Next** in the Welcome screen, select **Manual input** and click **Next**. Now you must enter the name for the custom group in 'User name' and enter the LDAP search query in 'Email address'. For instance if you wish to import users located in the Manchester office of the company bloggs.com you can enter `Manchester Group` in the user name and enter the following LDAP query in the Email address field:

```
<LDAP://CN=Users,DC=bloggs,DC=com>;(&(objectclass=user)(l=Manchester);distinguishedName;subtree)
```



The LDAP query is split into four sections separated by a semi colon (;).

1. The LDAP search root (required), for instance `<LDAP://CN=Users,DC=bloggs,DC=com>`.
2. The query filter (optional), for instance: `(&(objectclass=user)(l=Manchester)`; this filters all users from the city of Manchester (see tip below on how to test the query filter).
3. The return attribute (optional): this part specifies what attribute should be returned by the query and must be set to `distinguishedName`.
4. The search scope (optional): this part specifies whether subcontainers must be searched. To search subcontainers enter `subtree`. To only search the specified container excluding subcontainers, enter `onelevel`.

Note

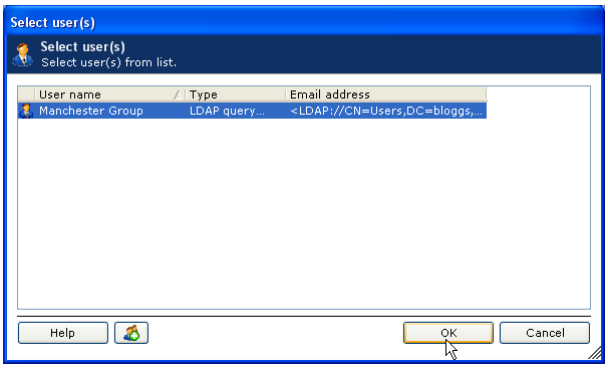
Note that the LDAP query must not exceed 120 characters.

For further assistance with creating your query, please send an email to support@redearthsoftware.com.

Tip

You can test your query filter (see point 2 above) in Active Directory to make sure it works correctly. To do so, open your Active Directory, right-click on your domain name, and select 'Find'. Now select 'Custom Search' from the 'Find:' drop-box, select the Advanced tab and enter your LDAP query filter, for instance (objectclass=user). Note that you should not enter the LDAP search root (see point 1 above) when testing your query filter in Active Directory. However you do have to enter the LDAP search root when entering your LDAP query in Policy Patrol.

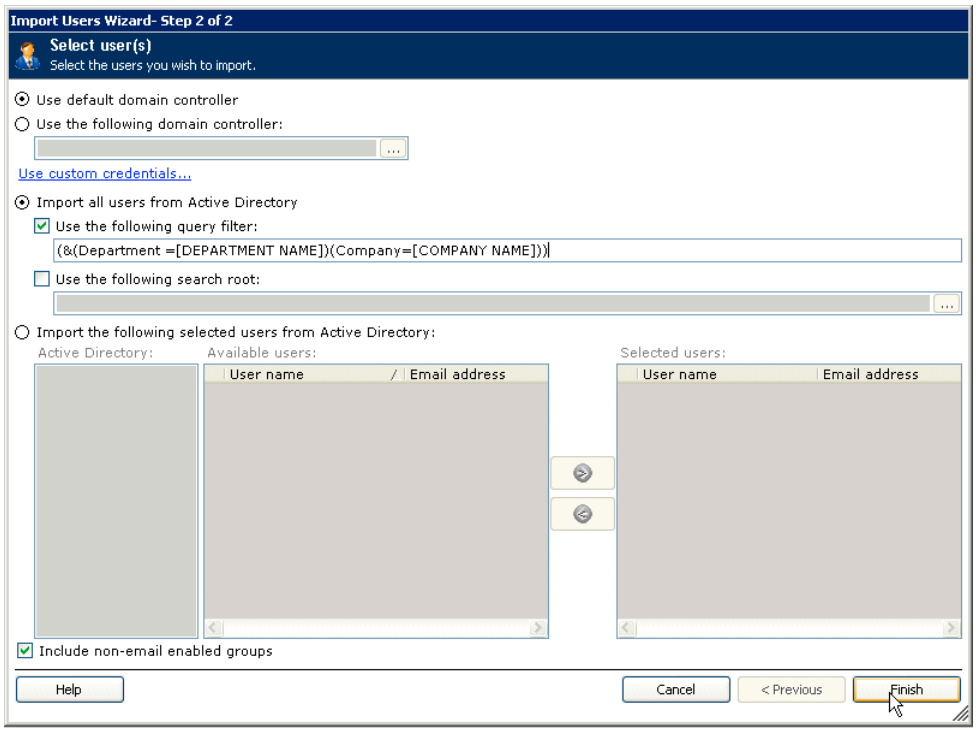
When you are ready, click **Finish**. The group name (i.e. Manchester Group) will now appear as a user when selecting users in a policy. By selecting the user 'Manchester Group' you will apply the policy to all users that are found by the query.



Remember however that you still need to license the users in Policy Patrol by importing them from Active Directory, Lotus Domino or by making use of manual input.

4.5 Using a Query filter to License Users

If you are importing users from Active Directory or Lotus Domino, you can configure a custom query filter that imports all users that have a certain Active Directory or Lotus Domino attribute. To do this, click on **Add** in **Settings** > **Users**. Click **Next** in the Welcome screen and select **Active Directory or Lotus Notes/Domino**. Tick the option **Use the following query filter** and enter the LDAP query.



For instance if you only wish to license users from a certain department you can enter the query as follows:

(Department=[DEPARTMENT NAME])

[DEPARTMENT NAME] is the value that is in the Active Directory Department field. For instance: `(Department=Marketing)`. It is also possible to create more advanced queries with AND (&) or OR (|). If you want two properties to be present, enter the query as follows:

(&(Department =[DEPARTMENT NAME])(Company=[COMPANY NAME]))

For instance, for users with Division 'Marketing' and company 'Bloggs & Co', enter: `(&(Department=Marketing)(Company=Bloggs & Co))`. If you want either property to be present, enter the query as follows:

(|(Department =[DEPARTMENT NAME])(Company=[COMPANY NAME]))

For instance for users with Division 'Marketing' or company 'Bloggs & Co', enter: `(|(Department=Marketing)(Company=Bloggs & Co))`.

You can also use an LDAP query to retrieve only the local users on the Exchange server, for example:

(homeMTA=CN=Microsoft MTA, CN=SERVER,CN=Servers,CN=First Administrative Group,CN=Administrative Groups, CN=Red Earth Software,CN=Microsoft Exchange, CN=Services, CN=Configuration,DC=redearth, DC=com)

The homeMTA string can be found in ADSI Edit (adsiedit.msc) by checking the homeMTA property of one of the users on the Exchange server. For more information on how to enter LDAP queries, please send an email to support@redearthsoftware.com.

Tip

You can test your query filter in Active Directory to make sure it works correctly. To do so, open your Active Directory, right-click on your domain name, and select 'Find'. Now select 'Custom Search' from the 'Find:' drop-box, select the Advanced tab and enter your query filter, for instance (objectclass=user).

Note

Note that the LDAP query must not exceed 120 characters.

When you have entered the query, click **Finish** to add the users to the licensed users list.

Note

If you want to apply a policy to users with a certain Active Directory or Lotus Domino attribute, you can do so by creating a group via the Manual input method and applying the rule to this group. For more instructions, please consult paragraph 4.4.2 'Creating a group based on an LDAP query'.

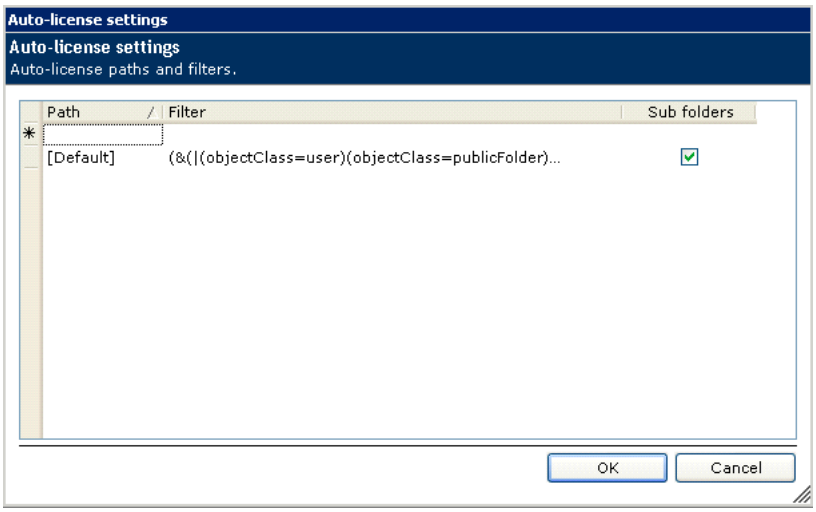
4.6 Editing Licensed Users

In **Settings** > **Users** a list of all licensed users is displayed. If you want to remove licensed users, you can select the user(s) and click on the **Remove** button. Alternatively you can import more users by clicking on **Add**. To edit the name or email address of a user, select the user and click on **Edit**. Make the necessary changes and click **OK**.

4.7 Auto-Licensing

If you wish Policy Patrol to automatically add and license new users, tick the option **Enable auto-licensing of new users**. This means that when a new user sends an email for the first time, the user will be licensed and any policies applying to all users or groups that the user is a member of (if the option **Include non-email enabled groups** is ticked), will be automatically applied.

Note that Policy Patrol will only auto license new users that are located in the paths that are listed in **Auto-license settings**. By default Policy Patrol lists the paths you used to import your users (including the sub tree of the specified path). So if you import users from only one OU, Policy Patrol will list only the path for users from that OU.



If you wish to change these paths, click on **Auto-license settings**. A dialog will be shown displaying the current paths that Policy Patrol uses for auto licensing. You will be able to edit, remove and add new paths. Auto licensing will only add new users that send emails out from the Policy Patrol machine that are found in one of these paths.

Note

Note that if you select the option **Enable auto-licensing of new users** you must make sure that you have purchased enough licenses to cover your users. If you do not have enough licenses, Policy Patrol will not license the new user and emails for this user will not be filtered. If this happens the Administrator will receive a notification by email, warning that more licenses need to be added. A warning message will also be shown in the Administration console.

4.8 Verify Users and Groups

If you move users, groups or objects in the Active Directory their location will automatically be updated in Policy Patrol. However, in case you would like to initiate this process manually, this can be done by clicking on the **Verify users/groups** button. If a user can no longer be located in the Active Directory, a dialog will pop up asking whether you wish to remove this user from licensing.

Chapter 5

Email Threat Protection

Policy Patrol offers Advanced Email Threat Protection to protect your organization from known and unknown threats and provides advanced features for blocking spam and unwanted emails, as well as detecting and preventing viruses & malware.

5.1 Configuring Email Threat Protection

Policy Patrol's Email Threat Protection protects your organization from spam, phishing, malware, and dangerous attachments. You can switch each option on or off from this dialog:

- Anti-Spam
- Anti-Phishing
- Anti-Malware
- Attachment Sanitization

Before you enable an option, you must go to the respective node and configure the relevant options. When you are done, go back to the Email Threat Protection mode and enable the option. By default Anti-Spam and Anti-Phishing have already been configured and are enabled if you selected to do so during the installation.

5.2 Threat Classifications

Policy Patrol groups emails into Threat Classifications in order to classify email messages and determine how the message should be handled. For instance Policy Patrol includes two threat classifications for spam messages: known spam and suspected spam. By making a distinction between known and suspected spam, you can concentrate only on a smaller amount of suspected spam, without wasting time sifting through a large number of spam messages that are already known to be spam.

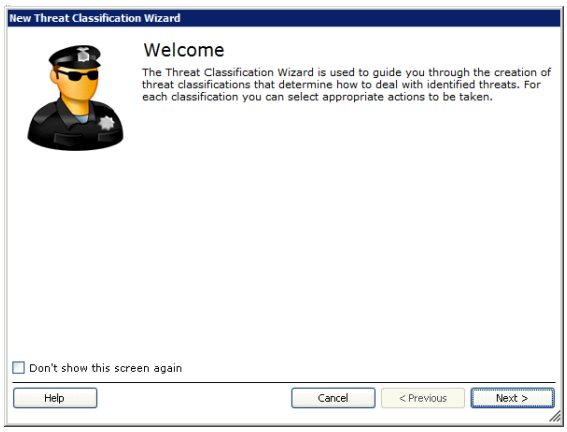
By default, Policy Patrol is already configured with a number of classifications. If required, you can change the classifications or create your own classifications.

5.2.1 Creating Threat Classifications

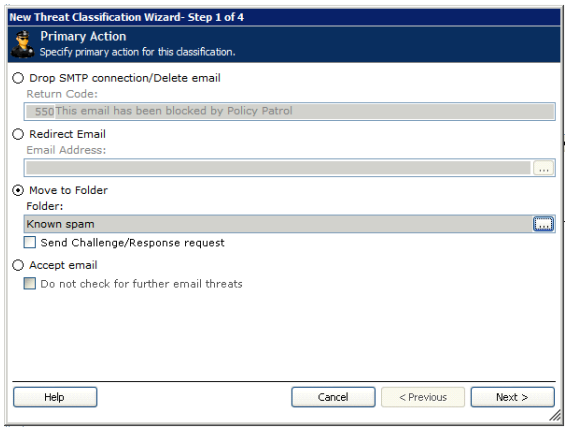
To create a new Threat Classification, follow the next steps:

1. Go to **Email Threat Protection** and click **New**.

2. The Threat Classification wizard will start up. Click **Next** in the Welcome screen.



3. Now select the primary action that should be taken for this Threat Classification.



The following primary actions are available:

Drop SMTP connection/Delete email: If you select this option Policy Patrol will either drop the connection (if applicable) or delete the message. Policy Patrol will drop the connection (in other words not download the message) for the checks that are done before the message is actually received (e.g. DNSBL, IP addresses, Address verification, Email block lists, Phishing block list and IP address block lists). This means that the message will never reach your mail server and hence will not use any bandwidth. If you wish you can change the response to the sending mail server by editing the return code and message. For all other checks that are performed after downloading the message (Word block list, spam characteristics and Bayesian filtering), Policy Patrol will delete the message.

Note

If Policy Patrol is installed behind a DMZ, the program will resolve the IP address of the relay server and not the original sender of the mail. Therefore Policy Patrol also checks the

previous IP addresses in the message headers for known spammers. However this can only be done after the message is actually received. Consequently, if Policy Patrol is installed behind a DMZ, Policy Patrol will delete messages instead of dropping the SMTP connection. Note that you must exclude the IP address of the forwarding DMZ machine in Anti-spam > Exclusions > Properties >DMZ, since this will save unnecessary lookups every time the DMZ forwards a message to the Policy Patrol machine.

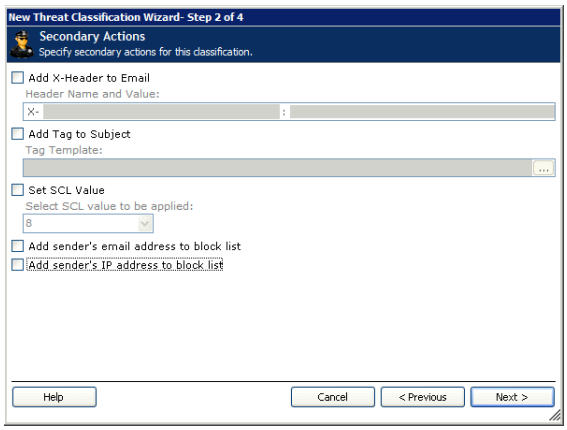
Redirect Email: Select this option to redirect the message to another mailbox. Enter or select the email address to redirect the messages to.

Move to Folder: Select this option if you wish to quarantine the message in a monitoring folder. Select the appropriate folder by clicking on the **...** button. If you wish to send a challenge/response message, tick the option **Send challenge/response request**. When the sender verifies the email, the message will automatically be released out of quarantine and delivered. Note that you must configure Challenge/Response for this (see paragraph 9.6 'Challenge/Response').

Accept Email: Select this option if you wish to accept the message and apply only the secondary action(s). Policy Patrol will continue processing the message to verify whether it belongs to another threat classification. If you do not want Policy Patrol to perform any further checks on these messages, you must check the option **Do not check for further email threats**. For instance if you simply want to deliver the message with a tag added, you can select this option.

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

4. Now you must select which secondary actions should be taken (if any):



Add X-Header to Email: If you select this option Policy Patrol will add an X-header to the message. Enter the header name and value you wish to add, for instance `X-PP-KNOWN-SPAM : TRUE`.

Add Tag to Subject: This option will add a tag to the subject. Select the tag template to be used by clicking on **...**.

Set SCL Value: This option will assign an SCL value to the message that Outlook can use to determine what action to take for the message. The SCL value can be from 0-9, with 0 indicating a legitimate message and 9 indicating a spam message. The value -1 indicates that the message is on the Allow List. It is also possible to increase the SCL value with a value from 1 to 9. To do this, select one of the options **Increase by n**, where n is the number to increase the value by. This can be useful if you are for instance using spam filtering on Exchange Server that adds an SCL value and you want to use Policy Patrol as an additional anti spam layer. If Policy Patrol considers the message spam, it can for instance increase the SCL value with 3. If the message already had an SCL value of 4, the new SCL value will be 7.

Add sender's email address to block list: Select this option to add the sender's email address to the block list.

Add sender's IP address to block list: Select this option to add the sender's IP address to the block list.

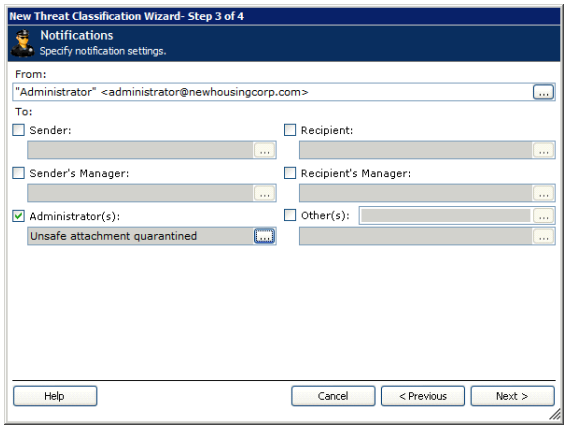
When you are ready configuring secondary actions click **Next**.

5. In this dialog you can configure any email notifications that you would like to be sent.

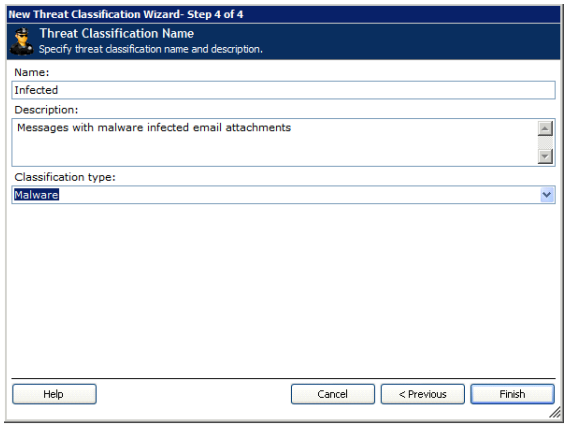
   Enter or select a From: address. If you wish a display name to appear in the notification message, enter "Display name" <email address>, e.g. `"John Doe" <John.Doe@company.com>`. Now specify who should receive the notification (Sender, Recipient, Administrator, Sender's Manager, Recipient(s)' Manager or Other(s)) and select the template to be used for each recipient. If you wish to use a new template, click **New...**. When you are done, click **Next**.

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> > Advanced > System configuration > System notifications.

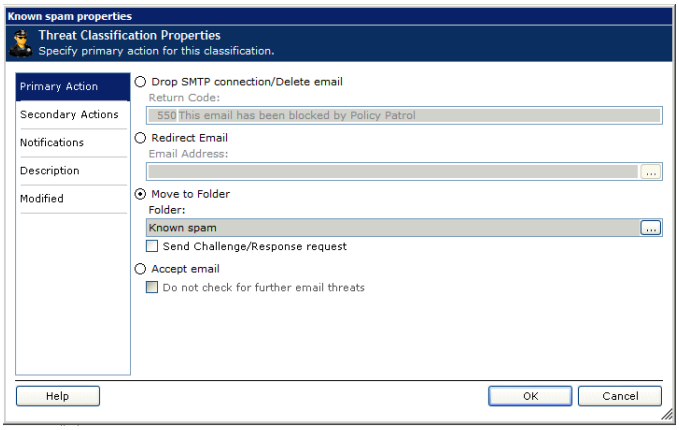


6. Enter a name and description for the classification. Select the Classification type for the classification. The type you select will determine how the message is counted and displayed in the Dashboard. When you are ready, click **Finish**.



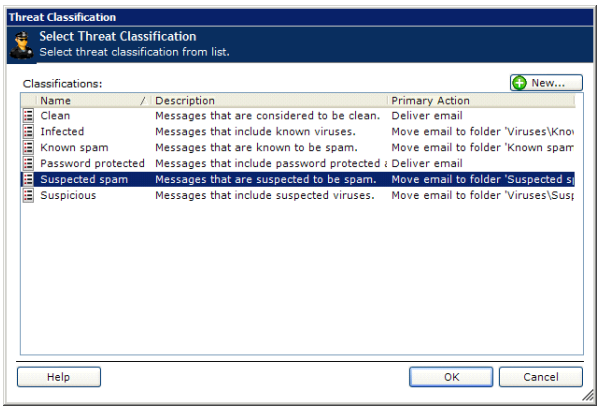
5.2.2 Editing Threat Classifications

To edit a Threat Classification, double-click on the Threat Classification or select the Threat Classification and click on the **Edit** button. A tabbed dialog will appear. To edit the Threat Classification, make the necessary changes and click **OK**.



5.2.3 Applying Threat Classifications

For each Email Threat Protection method you can select which Threat Classification should be applied. For instance you can select the Suspected spam classification for the Word Block List and the Known spam classification for the Email Block List.



By default Policy Patrol is pre-configured with six classifications (Infected, Known spam, Password protected, Suspected spam, Suspicious, and Clean), and these classifications are applied to each Email Threat Protection method as follows:

Threat Detection Method	Threat Classification
SPF record hard fail	Known spam
DNSBL lists	Known spam
SURBL lists	Known spam
Email block lists	Known spam
Phishing block list	Known spam
IP address block list	Known spam
Malware infected email attachments	Infected
SPF record soft fail	Suspected spam
Bayesian filtering	Suspected spam
Spam characteristics	Suspected spam
Character sets	Suspected spam
Words block list	Suspected spam
Verify MX record	Suspected spam
Verify SMTP connection	Suspected spam
Suspicious email attachments (anti-malware)	Suspicious
Password protected email attachments	Suspicious
Spoofed File Types	Suspicious

ⓘ Info

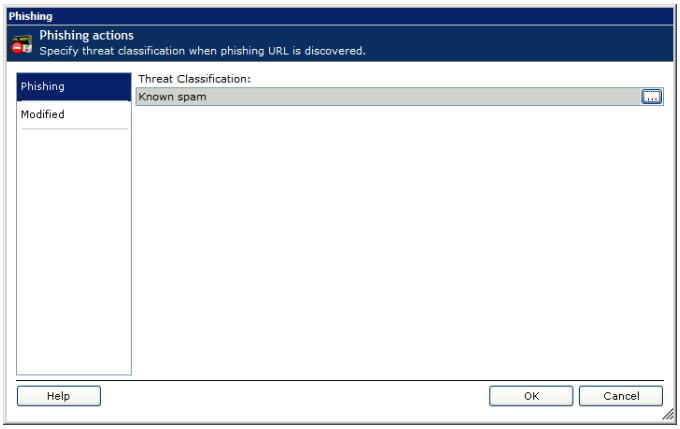
Note that you cannot select a threat classification for Greylisting (in the Anti-Spam node) or Address verification > Email Harvesting Protection. This is because these methods reject messages before they are downloaded and therefore Policy Patrol cannot perform any other actions on the messages.

5.3 Anti-Spam

Anti-Spam configuration settings are described in chapter 6.

5.4 Anti-Phishing

Policy Patrol includes a real-time anti-phishing block list in order to block phishing emails. In order to enable Anti-Phishing, click on **Threat classification for phishing**, select the appropriate Threat Classification and enable the option in the Email Threat Protection.



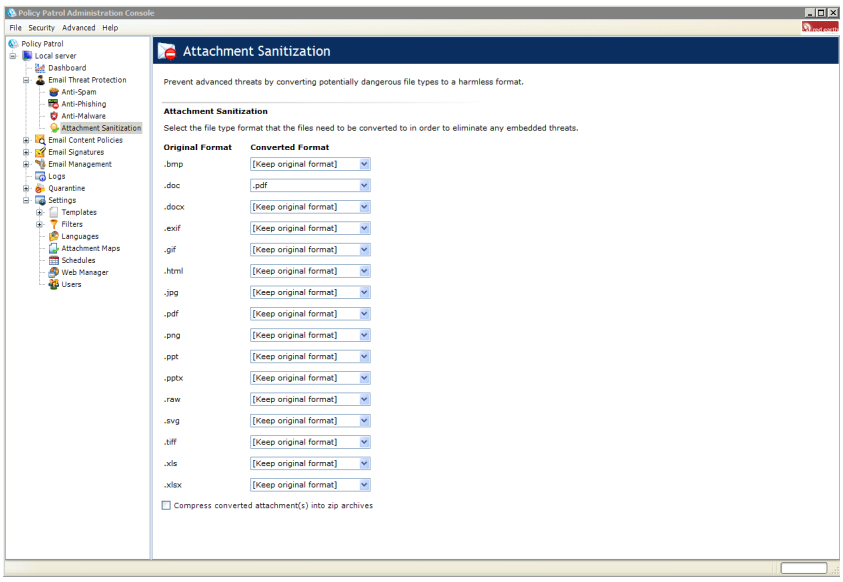
5.5 Anti-Malware

Anti Malware configuration settings are described in chapter 7.

5.6 Attachment Sanitization

To prevent advanced threats that might be missed by anti-malware engines, Metascan can sanitize potentially dangerous file types, thwarting zero-day and targeted attacks by converting to a different file type (e.g. DOC to PDF) to eliminate any embedded threats.

Note that in order to use Attachment Sanitization you must install Metascan on-premise on the same machine as Policy Patrol (see Chapter 7 Anti-Malware).



To configure Attachment Sanitization:

1. Go to **Email Threat Protection** and check the box **Attachment Sanitization**.

2. Go to **Attachment Sanitization** and select the **Converted Format** for the attachments that you would like to sanitize. For instance, if you would like to convert .doc files to pdf format, select .pdf in the Converted Format drop down box next to .doc. If you do not want to convert a file type, leave `[Keep original format]` selected for that file type.

3. Select the checkbox **Compress converted attachment(s) into zip archives** if you want to zip the attachments after they have been converted to the new file type.

Chapter 6

Anti-Spam

Policy Patrol combines several spam filtering methods to effectively block spam while ensuring a low false positive rate. These features can be configured from the Email Threat Protection > Anti Spam node in the Policy Patrol Administration console.

6.1 Stop Spam Right Out of the Box

Policy Patrol Mail Security is preconfigured to stop spam right out of the box (if you selected to enable spam filtering during installation). By default the program makes a distinction between Known spam and Suspected spam. The advantage of this is that it allows you to only focus on suspected spam messages and not waste time on known spam.

Known spam: placed in the Known spam folder and is deleted after 7 days.
Suspected spam: placed in the Suspected spam folder and is deleted after 15 days.

Tip

It is advisable to let each user review their own suspected spam. To remind users to check their suspected spam messages you can configure a daily quarantine report that can be emailed to each user, containing any newly quarantined messages. The user will be able to view the messages and deliver any wrongly quarantined items. They will also be able to update Allow Lists and Block lists. For instructions on how to configure the quarantine report, please go to Chapter 13.

6.1 Allow Lists

Policy Patrol includes Allow Lists to allow messages through the filter.

Policy Patrol includes an Email, Word and IP Address Allow List. If a sender is found in the Email Allow List or IP address Allow List, or if an email message meets the configured word score threshold from the Word Allow List, the email is allowed through and no further spam checking is performed. The email is also given a Spam Confidence Level (SCL) value of -1, which means that the email is on the Allow List.

6.1.1 Email Allow List

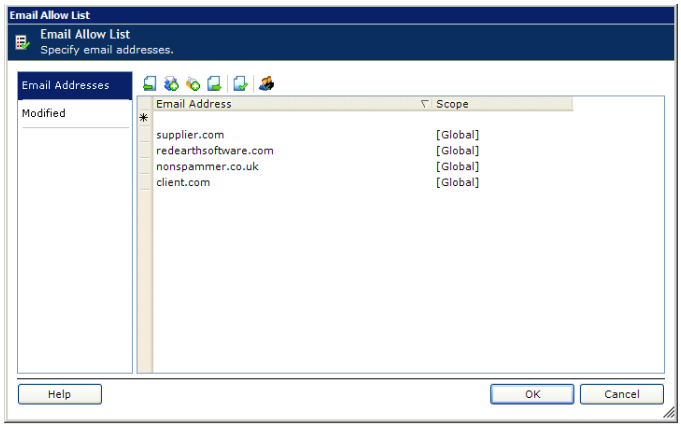
The Email Allow List contains sender email addresses and domains that must always be allowed through. You can also automatically add recipients of outgoing mails to the Allow List, excluding non-deliverable messages and out of office replies. To do this, enable the option **Enable automatic learning from outgoing mail**.

Policy Patrol considers email addresses in the Exchange 2007/2010/2013 'Safe senders' and 'Safe recipients' lists as part of the allow list and will let messages to the Safe recipients list and messages from Safe senders through without further checking. For more information on how to configure your Safe senders list consult this article: http://blogs.technet.com/b/exchange/archive/2011/07/08/accepted-domains-safe-senders-list-and-you.aspx

To manually add email addresses to the allow list:

1. Go to **Email Threat Protection** > **Anti-spam** > **Allow** tab.

2. Click on the **Email Allow List** button. 

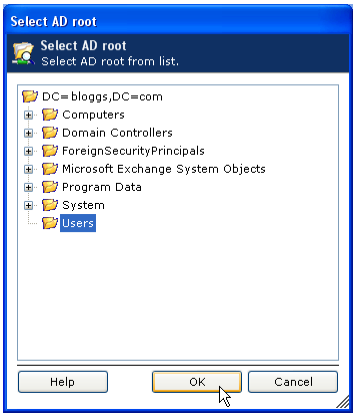


3. Enter the email addresses for the Allow List. If you wish to add a domain, you can simply enter the domain, there is no need to use a wildcard. For instance, if you wish to enter redearthsoftware.com in the Allow List, you must enter `redearthsoftware.com`. You can also use wild cards such as * and ?, although it is best to limit the number of wild cards to optimize performance.

   For each entry the **Scope** is specified. A [Global] Scope indicates that this entry is applicable for all users. If the entry is only applicable for certain users, the user name(s) for which it applies will appear in the Scope column. To allow individual users to only add email addresses to their own allow or block lists from the Web Manager, go to **Settings** > **Web Manager options** and select the option **Use individual email allow/block lists**. Note that when an Administrator adds an email address to the Allow List or Block List, it will always have `[Global]` as the scope.

   Import Active Directory Contacts: To import Active Directory contacts, click on the  icon in the toolbar. A dialog will pop-up asking you to select the AD root from where to

retrieve the contacts from. Make your selection and click **OK**. The contacts will now be added to the Allow List.



When you are ready entering email addresses, click **OK**.

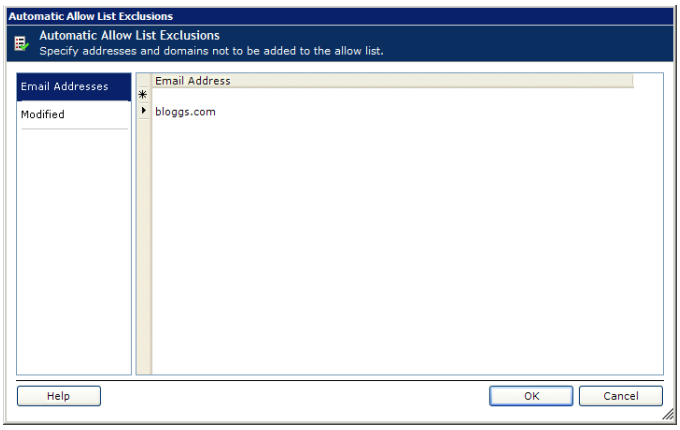
Info

You can also add entries to the Allow List from the monitoring folders or Message history in the Administration console. In addition, users & Administrators can add email addresses to the Allow List from the Policy Patrol Web manager (see chapter 13 Quarantined messages).

Import email addresses from Sent Items folder: To import the recipients from the Sent Items folder, click on the **Import from Sent Items** icon in the toolbar. A dialog will pop up asking you to select a user. Select a user and click **OK**. Policy Patrol will now import all external recipients from the user's Sent Items folder into the Allow List.

6.1.1.1 Email Allow List Exclusions

In order to prevent the wrong email addresses from being added to the Allow List (either by users or through automatic learning) you can enter email addresses to be excluded from the Allow List by clicking on the **Exclusions** button. For instance it makes sense to exclude your local domains from this list. If your local domains end up in the Allow List, this will let messages through that have a spoofed sender address with your domain. Note that the exclusions list overrides the entries in the Allow List. In other words if your local domain is entered in the Allow List as well as the exclusions list, the domain will not be considered to be on the Allow List.



6.1.2 Word Allow List

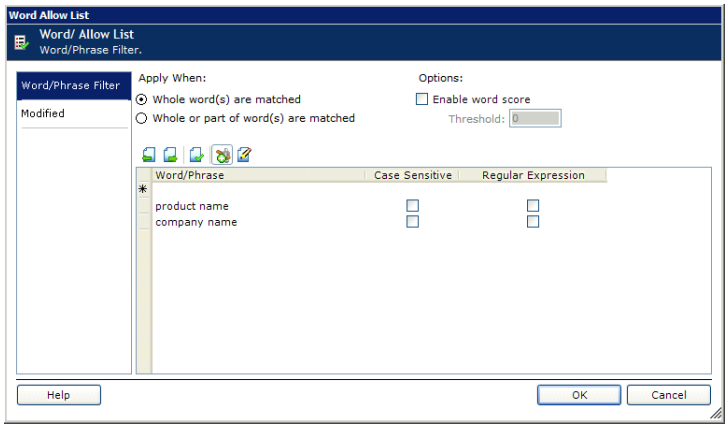
If a message contains words from the Word Allow List, the message will always be allowed through (with the exception of greylisting, recipient verification, Phishing block list and DNSBL – see note below). For instance, you could include your company name and your product/service names in the Word Allow List.

Note

If a message is blocked by greylisting, recipient verification, phishing block list or DNSBL the Word Allow List will not apply since these email threat checks are completed before the message is actually downloaded.

To add words to the allow List:

1. Go to **Email Threat Protection** > **Anti-spam** > **Allow** tab.
2. Click on the **Word Allow List** button. 
3. Enter the words and phrases to be included in the filter.



4. The following options are available:

Case Sensitivity
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.

Regular Expression
To view this option, click on the toolbar button 'Toggle advanced options'. If the entry is a regular expression tick the box **Regular Expression**. Regular expressions allow you to match a word pattern instead of an exact word. More information about how to configure regular expressions can be found in the following document:

Using Regular Expressions in Policy Patrol
(http://www.policypatrol.com/assets/pp10-regularexpressions.pdf)

Word Score
If you wish to use word score you must check **Enable Word Score**. For each word you will now be able to apply a word score. In the **Threshold** dialog box, specify the word score threshold that must be met to trigger the Allow List. You can also apply a negative word score. If you do not enable word score, messages that include one or more of the allowed words will be let through.

Multiple Count
If you enable word score, the multiple count option will also appear. If you wish every instance of the word to be counted, check the box **Multiple Count**. For example, if this box is enabled and you receive an email message that contains your company name three times, and you applied a word score of 5 to this word, the total word score would be 15. If you did not check this box, the word will only be counted once and the total score would be 5.

Apply when
You can 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. For instance, if you select that **Whole or part of word(s) are matched** and you enter your company name 'BloggsCo' in the filter, this will also include your website 'www.bloggsco.com' and email address 'person@bloggsco.com'. If you select **Whole word(s) are matched**, only your company name will be found, not your website and email address.

Note

Remember to select the option **'Whole words are matched'** since if your company name appears in your domain name, many spam mails will get through because they include the recipient's email address in the subject or body of the email message. For instance, if your company name is Bloggs and your domain is bloggs.com and you do not select the option Whole words are matched, Policy Patrol will let through all messages that include the email address in the subject or body.

Import/Export

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[TAB]Case sensitive[TAB]Regular expression[TAB]Score[TAB]Multiple count. The word/phrase and score values must be entered. For the other options, either 1 (enabled) or 0 (disabled) must be entered. For instance, if you wish to add the case sensitive word CLICK HERE with a word score of 5 and multiple count, you must enter it in the text file as follows:

```
CLICK HERE      1      0      5      1
```

For every word or phrase you need to start a new line. To export the words in the filter, click **Export**, enter a file name and select **OK**.

Remove Duplicates
If you wish to remove duplicates in the filter, click on the remove duplicates button in the toolbar.

6.1.3 IP Address Allow List

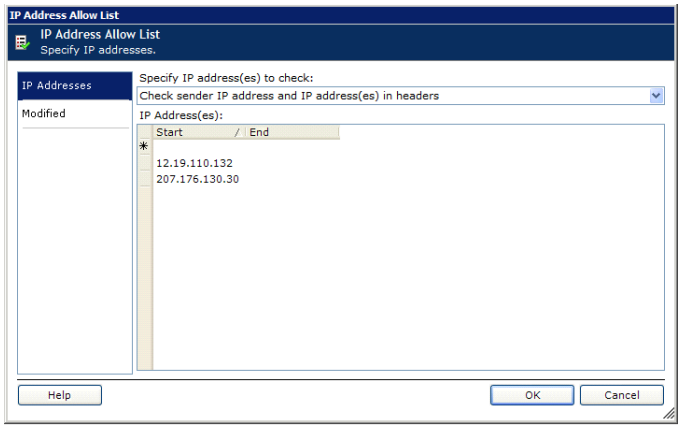
The IP address Allow List includes IP addresses from which messages will always be let through. To enter IP addresses in the Allow List:

1. Go to **Email Threat Protection** > **Anti-Spam** > **Allow**.

2. Click on the **IP Address Allow List** button. .

3. Specify which IP addresses to check. By default the option **Check Sender IP address and IP address(es) in headers** is selected. You only need to change this if your Policy Patrol installation is behind a DMZ or not receiving messages directly from the Internet. In this case you must select the option **Check only IP address(es) in headers**. If you do not wish Policy Patrol to check the message headers for IP addresses and you are receiving messages directly from the Internet you can select the option **Check only Sender IP address**.

   Now you must enter the IP addresses to be added to the Allow List. If you wish to add a single IP address, only enter a Start IP address. To add an IP range, enter the start and end IP address. The entered addresses and all addresses in between will be included in the range. When you are ready, click **OK**.



6.1.4 Configuring DNSWL Allow Lists

DNSWL lists contain IP addresses from senders who are known to be extremely unlikely to ever send spam. These lists contain IP addresses from qualified corporations such as banks, accounting firms, law firms, airlines, medical centers, government agencies, and transactional mail from automated billing systems, ecommerce servers, online banking and booking systems.

To configure a new DNSWL list:

1. Go to **Email Threat Protection** > **Anti-spam** > **Allow** tab.

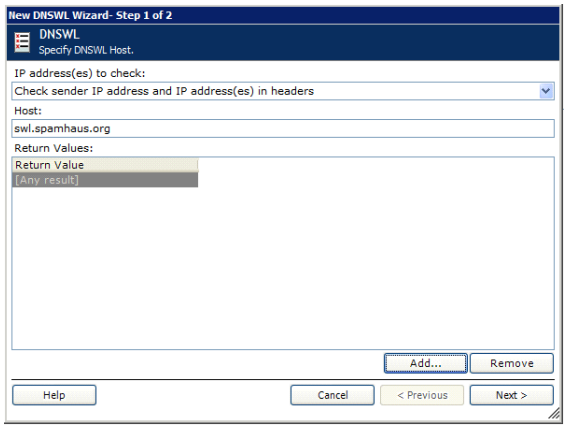
2. In DNSWL Lists, click on **New**.

3. Click **Next** in the Welcome screen.

4. Specify which IP addresses Policy Patrol must check. By default the option **Check sender IP address and IP address(es) in headers** is selected. You only need to change this if your Policy Patrol installation is behind a DMZ or not receiving messages directly from the Internet. In this case you must select the option **Check only IP address(es) in headers**. If you do not wish Policy Patrol to check the message headers for IP addresses and you are receiving messages directly from the Internet you can select the option **Check only Sender IP address**.

   Enter the **Host address** for the list. For instance for the Spamhaus allow list, enter `swl.spamhaus.org`.

   Click on **Add**. Select whether you wish to check for **All return values** or a specific return value, for instance `127.0.2.3`.



   Some allow lists don't use specific return values, i.e. if the allow list returns any value it means that the email address is listed on the allow list. In this case you should select **All return values**. If a list has multiple return values, such as the dnwsl.org list, you can click **Add** and enter the return value that you wish to treat as listed on the allow list. For instance for dnwsl.org, the return value 127.0.2.3 indicates a highly trustworthy financial services provider. Enter this return value and click **OK**. If you wish to enter more return values, click on **Add** again and repeat the process.

When you have entered all the return values, click **Next**.

5. Enter a name for the list and a description. If the list should be enabled, select **Enable this DNSWL entry**. Click **Finish**.

> **Note**
>
> Some DNS allow lists charge for commercial use. Please check the lists usage terms to find out if you need to purchase a license to use the list.

6.2 Block Lists

Policy Patrol includes an Email, IP address and Word Block list. If a sender is found on the block list or if an email message meets the configured word score threshold from the word block list, the messages are categorized as the selected threat classification.

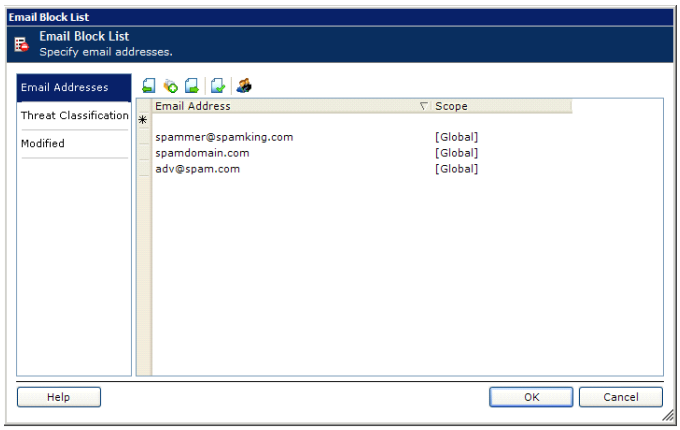
6.2.1 Email Block List

The email block list includes sender addresses that must be blocked. You can manually enter addresses and you can configure Policy Patrol to add addresses automatically (through threat classification actions). It is also possible for users and Administrators to add senders to the block list via the web manager and administration console.

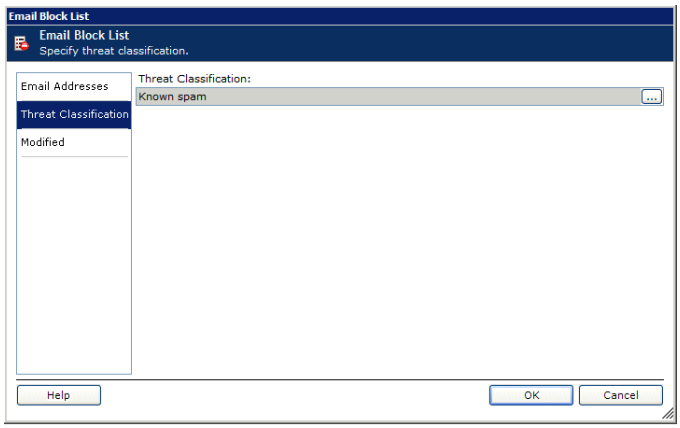
To manually add addresses to the block list:

1. Go to **Email Threat Protection** > **Anti-spam** > **Block** tab.
2. Click on the **Email Block List** button. 
3. Enter the email addresses for the block list. If you wish to add a domain, you can simply enter the domain; there is no need to use a wildcard. For instance, if you wish to enter spammer.com in the block list, you must enter `spammer.com`. You can also use wild cards such as * and ?, although it is best to limit the number of wild cards to optimize performance. When you are ready entering email addresses, click **OK**.

   For each entry the **Scope** is specified. A [Global] Scope indicates that this entry is applicable for all users. If the entry is only applicable for certain users, the user name for which it applies will appear in the Scope column. If the same email address has been added to the block list by multiple users for their individual lists, the email address will be listed separately each time with the respective user name in the scope. To allow individual users to only add email addresses to their own allow/block lists from the Web Manager, go to **Settings** > **Web Manager** and select the option **Use individual email allow/block lists**.



Now you must select the threat classification for these messages. To do this, go to the Threat Classification tab and select the threat classification from the list. By default the **Known spam** classification is selected.



Other ways to add email addresses to the block list:

- Automatically add senders of spam mails to the block list: To do this, you must select the secondary action '**Add sender's email address to block list'** for the threat classification. Note that since spammers continually change their email address, this is not really recommended.

- Add senders to block list from the quarantine folders: In the Policy Patrol Administration console or Web Manager you can add sender email addresses to the block list by right-clicking the message(es) and selecting Delete. A screen will pop-up allowing you to select block list options. The web manager also allows users and Administrators to manually add a new entry to the block list.

- Add senders to the block list from Logs: Go to the Logs node in the Policy Patrol Administration console or Web Manager (only for Administrators). Right-click the message and select **Block list**.

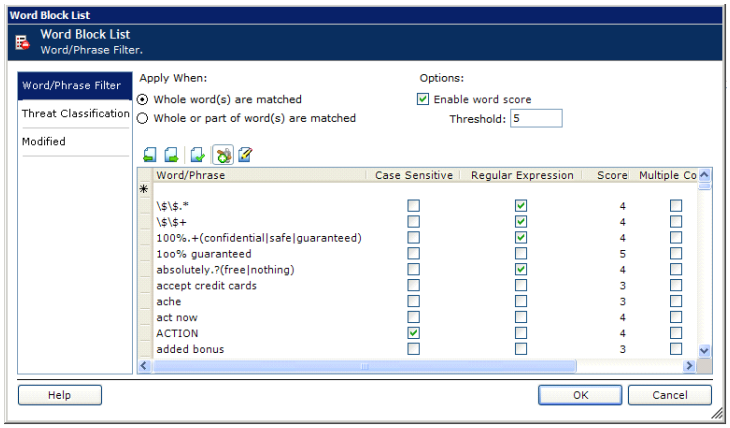
6.2.2 Word Block List

The Word Block List contains a list of words that if present in a message, indicate spam. Policy Patrol ships with a comprehensive block list of commonly used spam words (utilizing regular expressions). To enter more words and phrases on the block list:

1. Go to **Email Threat Protection** > **Anti-Spam** > **Block** tab.

2. Click on the **Word Block List** button. 

3. Enter the word(s) or phrases to be included in the filter. The following options are available:



Case Sensitivity
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.

Regular Expression
To view this option, click on the toolbar button 'Toggle advanced options'. If the entry is a regular expression tick the box **Regular expression**. Regular expressions allow you to match a word pattern instead of an exact word. This means that by making use of regular expressions you can stop spammers trying to circumvent content filters by adding characters within words, such as v*i*a*g*r*a or c-l-i-c-k h-e-r-e. You can also detect word variations such as r@tes and l0ans. Policy Patrol includes an extensive block list that makes use of many regular expressions to detect variations of spam words. More information about how to configure regular expressions can be found in the following document:

Using Regular Expressions in Policy Patrol
(http://www.policypatrol.com/assets/pp10-regularexpressions.pdf)

Word Score
If you wish to use word score you must check **Enable word score**. For each word you will now be able to apply a word score. This can be a positive word score, but also a negative word score. For instance, a negative score 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. In the **Threshold** dialog box, specify the word score threshold that must be met to trigger the Allow List. If a message reaches this word score, the specified actions will be taken. If you do not enable word score, the specified actions will be taken if any of the words in the list are found in the subject or body.

Multiple Count
If you enable word score, the multiple count option will also appear. If you wish every instance of the word to be counted, check the box **Multiple count**. For example, if this box is enabled and you receive an email message that contains the word 'debt' three times, and you applied a word score of 5 to this word, the total word score would be 15. If you did not check this box, the word will only be counted once and the total score would be 5.

Apply when
You can 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. 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 word 'sex' will trigger, but not 'Middlesex'.

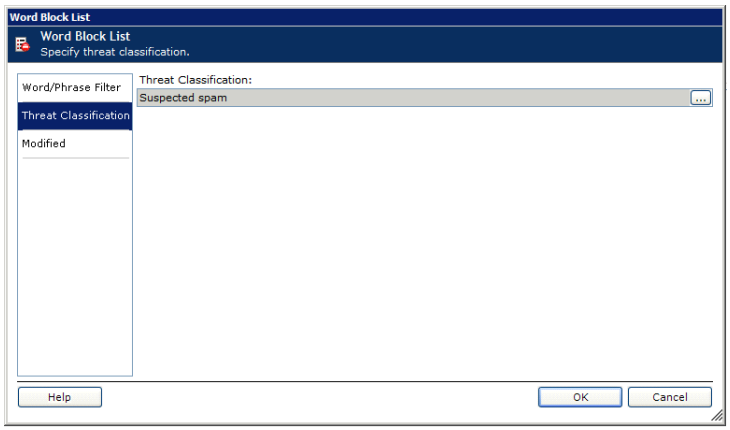
Import/Export
You can import lists from .txt files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. The format should be as follows: Word[TAB]Case sensitive[TAB]Regular expression[TAB]Score[TAB]Multiple count. The word/phrase and score values must be entered. For the other options, either 1 (enabled) or 0 (disabled) must be entered. For instance, if you wish to add the case sensitive word CLICK HERE with a word score of 5 and multiple count, you must enter it in the text file as follows: `CLICK HERE 1 0 5 1`. For every word you must start a new line. To export the words in the filter, click **Export**, enter a file name and select **OK**.

Remove Duplicates
If you wish to remove duplicates in the filter, click on the remove duplicates button in the toolbar.

More information on word/phrase filtering can be found in the following document:

How to configure word/phrase filtering
(http://www.policypatrol.com/assets/pp10-wordfiltering.pdf)

Now you must select the threat classification to be applied to messages that reach the word block list threshold. Go to the **Threat Classification** tab and click on the … to select the threat classification. By default the **Suspected spam** classification is selected.



6.2.3 IP Address Block List

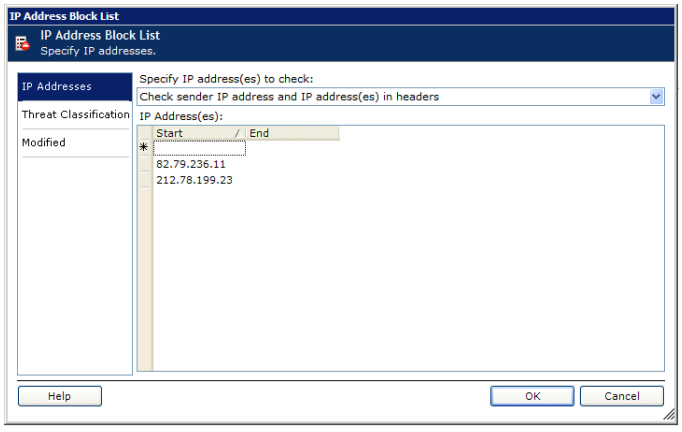
To manually add addresses to the IP address block list:

1. Go to **Email Threat Protection** > **Anti-spam** > **Block** tab.

2. Click on the **IP Address Block List** button. 

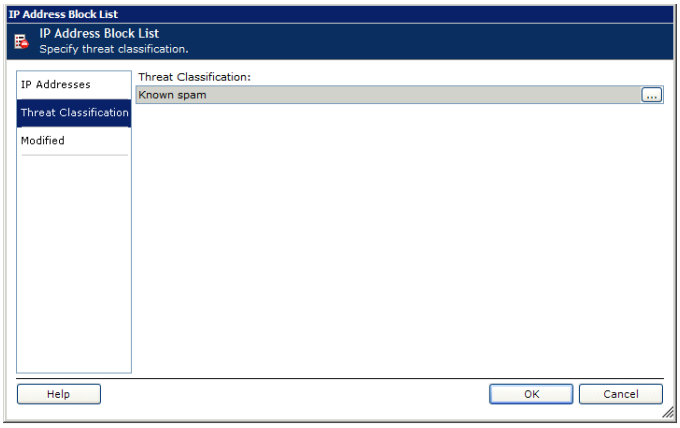
3. Specify which IP addresses to check. By default the option **Check Sender IP address and IP address(es) in headers** is selected. You only need to change this if your Policy Patrol installation is behind a DMZ or not receiving messages directly from the Internet. In this case you must select the option **Check only IP address(es) in headers**. If you do not wish Policy Patrol to check the message headers for IP addresses and you are receiving messages directly from the Internet you can select the option **Check only Sender IP address**.

   Now you must enter the IP addresses for the block list. Enter a single IP address in the Start column. If entering an IP range, enter the begin IP address in the Start column and the end IP address in the End column. When you are ready entering IP addresses, click **OK**.



To automatically add IP addresses to the block list for identified spam messages you must select the secondary action '**Add sender's IP address to block list'** for the threat classification. For instance you could select this for the **Known spam** classification.

Now you must select the threat classification to be applied to messages that are sent from these IP addresses. Go the **Threat Classification** tab and click on the … to select the threat classification. By default the **Known spam** classification is selected.



6.2.4 Countries Blocked

If you wish to block emails originating from certain countries, follow the next steps:

1. Go to **Email Threat Protection** > **Anti-spam** > **Block** tab > **Countries Blocked** top tab.

2. Click on **New**.

3. Click **Next** in the Welcome screen.

4. Select the countries you would like to block in the left pane and click on the right arrow. The selected countries will appear in the right pane. To deselect countries, click on the countries in the right pane and click on the left arrow. When you are done, click **Next**.

5. You will be asked to select a threat classification. Click on the Browse button, select a classification from the list and click **Next**.

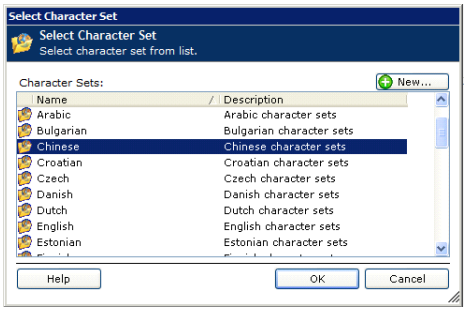
6. Enter a policy name and description and click **Finish**.

You can create multiple policies, for instance if you wish to treat emails from certain countries as suspect you can apply the Suspected spam classification to these emails. You can create another policy where you select countries from which emails need to be considered as Known spam.

6.2.5 Character Set Blocking

This option allows you to accept or block messages that use certain character sets. For instance, if you only want to accept emails that use the English character set, you can select the option **Accept only emails using the following character sets**. Then click on **Add** and select **English** from the list.

Important: If you select this option you must select the **Clean** Threat Classification by clicking on 'Specify threat classification' and in Threat Classification selecting the Clean classification.



If you wish to allow all messages apart from emails that for instance use Chinese or Korean code pages, enable the option **Accept all emails except those using the following character sets**. Then click on **Add** and select Chinese and Korean. Click **OK**.

If you want to add more languages you can do so from **Settings** > **Languages** (see chapter 'Settings').

Click on **Configure threat classification** in order to select the Threat Classification for messages that use the selected character sets. By default the threat classification is **Suspected spam**.

6.2.6 DNSBL Lists

Policy Patrol already includes a number of preconfigured DNS block lists (DNSBL), some of which are enabled by default. You can enable/disable the preconfigured lists, or you can add new ones.

ⓘ Info

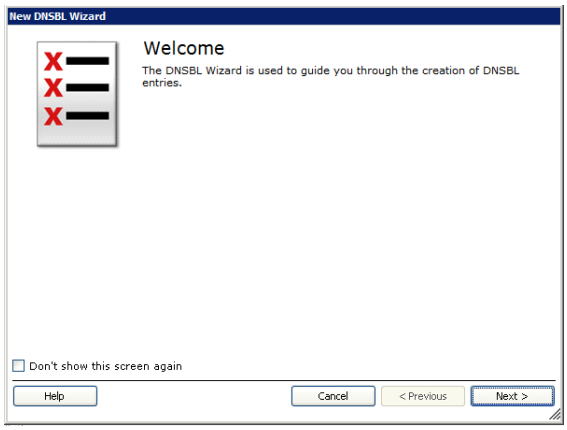
There are several DNS block lists that contain IP addresses from known spammers. Policy Patrol Email can use these lists to identify messages as spam before they are actually downloaded. How accurate this filtering is, depends on the list you use. There are two types of lists:

- Lists of known spammer's domains, for example the Spamhaus Block List (SBL) (http://spamhaus.org/sbl/)
- Lists of mail servers that are open to relaying and therefore will allow spammers to send mail via their mail server.

Whilst lists of the first type (spammer's domains) are 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 quarantine mails from open relay lists.

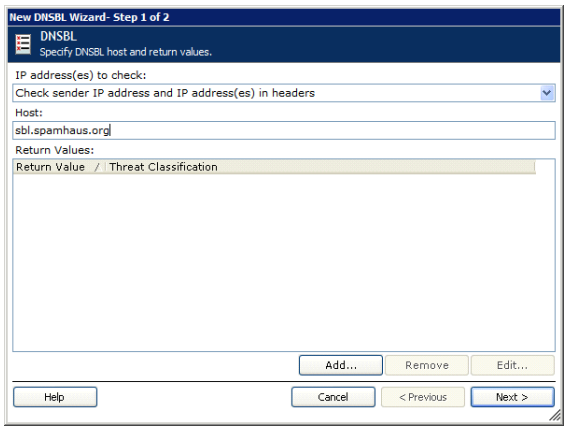
To configure a new DNSBL list:

1. Go to **Email Threat Protection** > **Anti-Spam** > **Block** tab > **DNSBL Lists** tab.
2. Click on **New**.
3. In the Welcome screen click **Next**.



4. Specify which IP addresses Policy Patrol must check. By default the option **Check sender IP address and IP address(es) in headers** is selected. You only need to change this if your Policy Patrol installation is behind a DMZ or not receiving messages directly from the Internet. In this case you must select the option **Check only IP address(es) in headers**. If you do not wish Policy Patrol to check the message headers for IP addresses and you are receiving messages directly from the Internet you can select the option **Check only Sender IP address**.

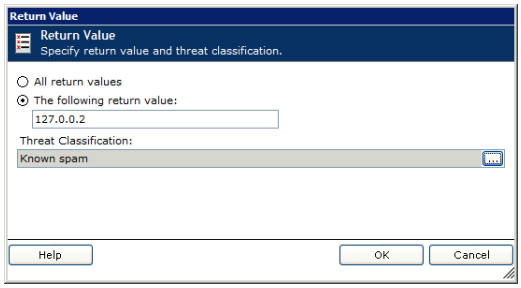
   Enter the **Host address** for the list. For instance for the Spamhaus Block List (SBL), enter `sbl.spamhaus.org`.



   Click on **Add**. Select whether you wish to check for **All return values** or a specific return value, for instance `127.0.0.2` for the Spamhaus Block List (SBL).

Tip

If you wish different actions to be taken per return value, you can add an entry for each return value and specify a different threat classification.

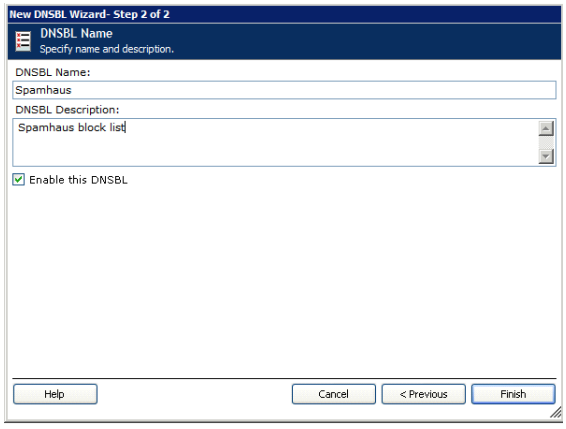


Now select the threat classification to apply these messages to. If the DNSBL list identifies known spammers, choose the Known spam classification. If the DNSBL list identifies open relays, select the Suspected spam classification.

If a list has multiple return values you can click **Add** and enter the other return values for the list. This allows you to take different actions according to the returns. For instance, the DNSRBL list (www.dnsrbl.com) has several returns. If the DNSRBL list returns 127.0.0.4, the site has been identified as a constant source of spam. Therefore you would want to select the **Known spam** classification for messages that return this value. However, if the list returns the value 127.0.0.5 this indicates that the site is a smart host. Since this might create more false positives, you would want to identify these messages as **Suspected spam** instead.

When you have entered all the return values, click **Next**.

5. Enter a name for the list and a description. If the list should be enabled, select **Enable this DNSBL entry**. Click **Finish**.

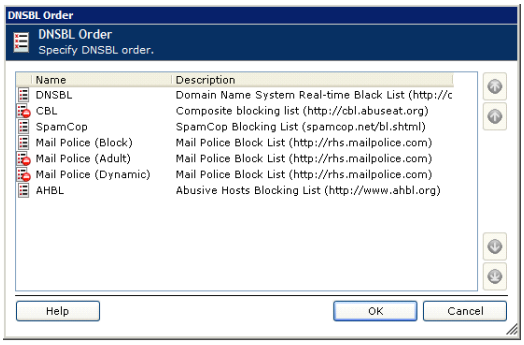


Note

Some DNS block lists charge for commercial use. Please check the lists usage terms to find out if you need to purchase a license to use the list.

6.2.6.1 Change DNSBL Order

To change the order in which Policy Patrol checks DNSBL lists, click on the **Order** button in the bottom right corner. Select the DNSBL list and use the up and down arrows to change the order of the list.



6.3 SURBL Lists

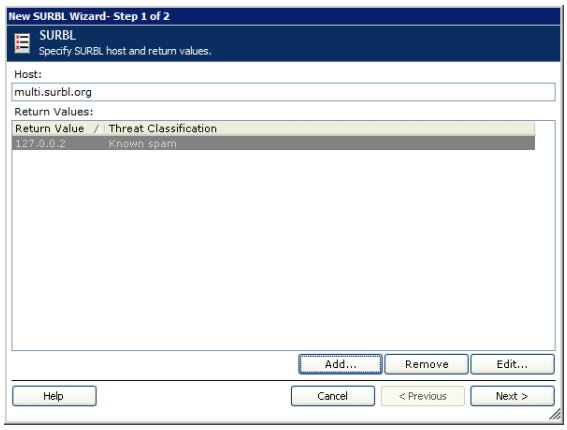
Policy Patrol can use SURBL Lists to check for known spammer URLs in the email message body. This means that messages will be checked after the message is downloaded; as opposed to RBLs and IP address ranges that are checked before the message is downloaded.

Policy Patrol includes a number of preconfigured SURBL lists. You can enable or disable the configured SURBL lists or you can configure your own. To configure a new SURBL List:

1. Go to **Email Threat Protection > Anti-Spam > SURBL** and click **New**.

2. In the Welcome screen click **Next**.

3. Enter the **Host address** for the list. For instance for the combined SURBL list enter `multi.surbl.org`. Click on **Add**. Select whether you wish to check for all return values or a specific return value, for instance `127.0.0.2`. The combined SURBL list can have many different returns, so to include all returns select **All return values**.



Tip

If you wish to apply different threat classifications per return value, you can add an entry for each return value and specify a different classification for each.

Now select the Threat Classification to apply to these messages. If the SURBL list identifies known spammers, choose the Known spam classification. If the SURBL list identifies suspected spammers, select the Suspected spam classification. Most SURBL lists will detect known spam messages.

When you are ready configuring actions click **OK**. If a list has multiple return values you can click **Add** and enter the other return values for the list. This allows you to take different actions according to the returns. When you have entered all the return values, click **Next**.

4. Enter a name for the list and a description. If the list should be enabled, select **Enable this SURBL entry**. Click **Finish**.

Note

Note that some SURBL lists charge for commercial use. Please check the lists usage terms to find out if you need to purchase a license to use the list.

6.3.1.1 Change SURBL Order

To change the order in which Policy Patrol checks SURBL lists, click on the **Order** button in the bottom right corner. Select the SURBL list and use the up and down arrows to change the order of the list.

6.4 Address Verification

Policy Patrol includes a number of address verification options to determine whether the sending mail server is legitimate or whether it has 'spam-like' attributes. Policy Patrol can also block email harvesting attempts by verifying recipients before accepting emails.

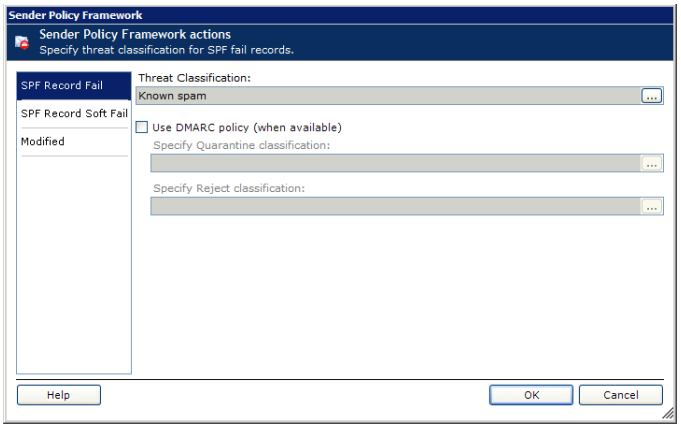
6.4.1 Sender Verification

6.4.1.1 Sender Policy Framework (SPF)

The Sender Policy Framework (SPF) allows you to verify whether the sender is actually who they say they are. This means that by using SPF, Policy Patrol can block spoofed emails and thwart phishing attempts. If you wish Policy Patrol to verify senders using the Sender Policy Framework, tick the option **Check sender's IP address in Sender Policy Framework (SPF)**. Policy Patrol will check the From: address before the message is downloaded and the Reply to: address after downloading the message.

Note

You cannot use Sender Policy Framework if Policy Patrol is installed behind a DMZ.



Click on the button  **Select threat classification for failed SPF checks** to specify the threat classifications for the failed SPF checks. Policy Patrol allows you to specify different classifications depending on the SPF response (if the sender is verified by SPF, the email is let through and subjected to further anti-spam checks). The dialog contains two tabs:

- **SPF Record Soft Fail**: A soft fail indicates that the message should be considered as suspicious. By default these messages are classified as Suspected spam (recommended).
- **SPF Record Fail**: A record fail means that the sender domain is spoofed and that the message can confidently be identified as spam. These messages are classified as Known spam by default.

6.4.1.2 DMARC Policies

DMARC stands for Domain-based Message Authentication, Reporting & Conformance. DMARC policies allow domain owners to specify how to handle emails that were spoofed as originating from their organization. For instance if Policy Patrol receives an email with customerservice@bankofamerica.com in the From: address that has been spoofed, Policy Patrol can take action on the message according to the DMARC policy set by Bank of America.

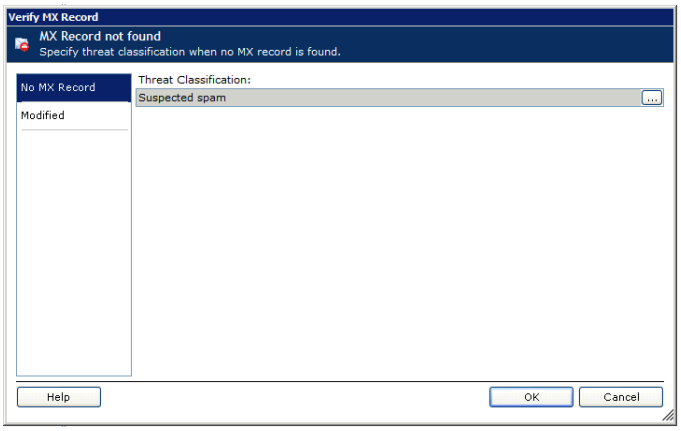
If you want to implement DMARC Policies, select the option **Use DMARC policy (when available)**. And select the threat classification for the DMARC policy 'Quarantine' and 'Reject'. In other words, if the domain owner specifies that they would like the email to be quarantined or rejected, select how the messages will be treated.

If you would like to set a DMARC Policy specifying how other organizations should handle spammers that spoof your domain, you can do this in your DNS settings.

By implementing DMARC policies and setting DMARC policies in your DNS settings, you can contribute to the reduction of email abuse.

6.4.1.3 Verify MX Record

If you enable the option **Verify existence of sender MX Record**, Policy Patrol will check whether the sending mail server has an MX record. In order to receive mail for a domain, you need to have at least one MX record. The mail servers that spammers use often do not have an MX record, since they do not need to receive emails and without an MX record they can remain anonymous and difficult to trace. Note however that some legitimate companies use separate mail servers for sending and receiving mail, where the sending mail server will not have an MX record. Therefore you must not treat these messages as known spam, only as suspected spam.



Click on the button to configure the threat classification for senders without an MX record. In the 'No MX Record' tab, select the threat classification by clicking on the **...** button. Select the threat classification from the list and click **OK**. To create a new threat classification, click on the **New** button.

6.4.1.4 Connect to Sender's SMTP Server

If you enable the option **Verify sender's SMTP Connection**, Policy Patrol will attempt to connect to the mail server(s) specified in the MX record of the sender's domain. Click on the button to configure the threat classification for senders with failed connections. In the 'Failed SMTP connection' tab, select the threat classification by clicking on the browse (**...**) button. Select the classification from the list and click **OK**. To create a new threat classification, click on the **New** button.

6.4.1.5 Limit Delivery Status Notifications

If you do not want to send non-deliverable messages to senders not listed in the Allow List, select the option **Only send Delivery Status Notifications (DSNs) to senders in allow list**.

6.4.2 Email Harvesting

Email harvesting prevents spammers 'guessing' email addresses by sending emails to a large number of email addresses in the hope that some addresses are correct. Email harvesting will detect the invalid recipients and will reject the messages before the messages are downloaded, therefore offering important bandwidth savings.

To reject messages that are not addressed to valid recipients, tick the option **Drop SMTP connection when x or more invalid recipient(s) are detected**. By default the number is set to 2. By enabling this option you can protect your mail server against email address harvesting and NDR spam attacks. You can also select to add the sender IP address to the block list, in order to block any future email harvesting attacks. To enable this, select the option **Add IP address to block list when dropping SMTP connection**.

If you wish to delay the response that Policy Patrol sends when a recipient is not valid, you can select the option **Delay recipient rejection responses** and select the number of seconds that the response should be delayed for. The delay can be useful to slow down an email harvest attack and to slow down spammers in general.

Note

Policy Patrol will only perform email harvesting protection for messages received from external IP addresses.

Info

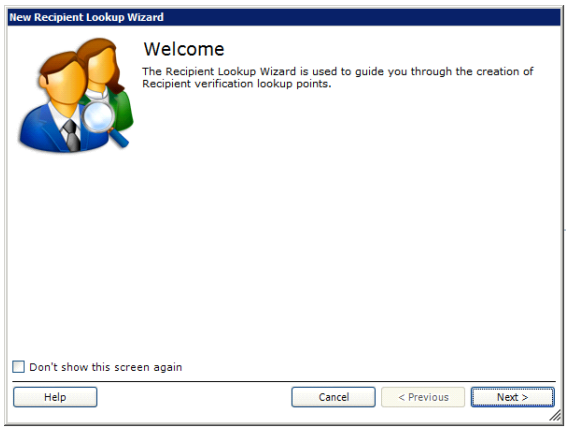
Address harvesting: In order to gather valid email addresses, spammers perform address harvesting by submitting SMTP requests for many different email addresses. If a valid response is received, the spammer knows that this is a live email address and can proceed to send spam to this email address. Address harvesting uses up bandwidth and produces more spam. Policy Patrol can protect against this by dropping the SMTP connection when it detects address harvesting.

NDR 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 to the sender, i.e. the spam victim, with the original spam message attached. With recipient verification enabled, Policy Patrol will simply reject these messages (i.e. not download them) and send an invalid address response to the sending mail server. This will cause the sending mail server to send an NDR message instead of your mail server, freeing up valuable bandwidth. Legitimate emails that have been

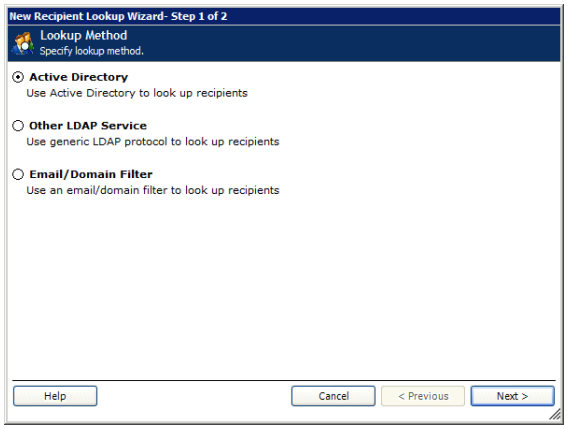
mistakenly addressed will still generate an NDR, however this NDR will not be sent by your mail server but by the sender's own mail server.

When you select the option **Drop SMTP connection when x number of invalid recipient(s) are detected** you will be asked to configure a recipient lookup point. Click **Yes** to configure a Recipient lookup point or click the **New** button.

1. In the Welcome screen click **Next**.



2. Specify where Policy Patrol must search for your recipient addresses. Select **Active Directory**, **Other LDAP service** (select this option if you have Lotus Domino without Active Directory) or **Email/domain filter**. Click **Next**.

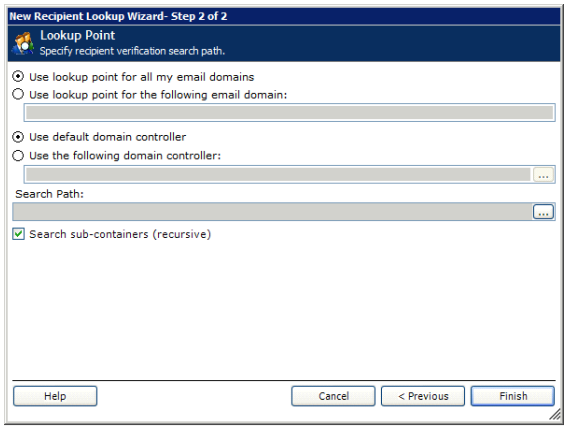


3. Now configure your lookup point:

   If you selected Active Directory

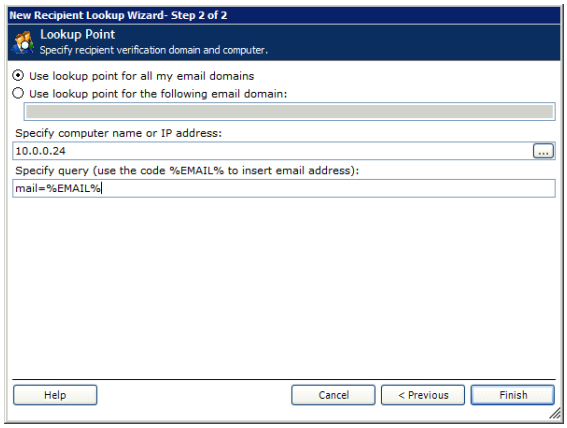
   If you want to use this lookup point for all your domains, select **Use lookup point for all my email domains**. If you want to specify different lookup points for different domains, select the option **Use lookup point for the following email domain** and enter the domain, i.e. `company.com`. Select whether you wish to use the default domain controller or another domain controller. In specify search path, select the Active Directory search root that

must be used to verify recipients. Note that all your users must be in this Active Directory search root (in the same domain). If not all users are in the search root, mails to these users will be rejected. Tick the option **Search sub-containers (recursive)** if you wish the sub containers to be searched as well. When you are ready, click **Finish**.



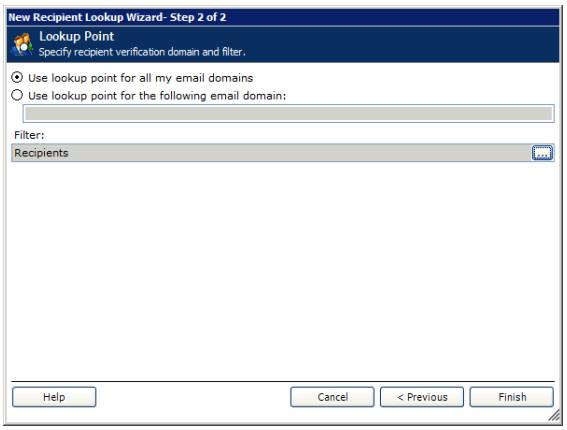
If you selected Other LDAP Service

If you want to use this lookup point for all your domains, select **Use lookup point for all my email domains**. If you want to specify different lookup points for different domains, select the option **Use lookup point for the following email domain** and enter the domain, i.e. `company.com`. Enter or select the computer name or IP address that Policy Patrol must access. Now specify the query that must be used, i.e. `mail=%EMAIL%` for Lotus Domino. When you are ready, click **Finish**.



If you selected Email/Domain filter

If you want to use this lookup point for all your domains, select **Use lookup point for all my email domains**. If you want to specify different lookup points for different domains, select the option **Use lookup point for the following email domain** and enter the domain, i.e. `company.com`. Select the filter that includes the valid recipients by clicking on the **...** button. To create a new filter, click on the **New ...** button above the filter list.



Repeat the steps above for every different lookup method you wish Policy Patrol to use.

Note

You must make sure that the recipient lookup points include all your valid recipients since Policy Patrol will reject messages that are not addressed to recipients included in your lookup points.

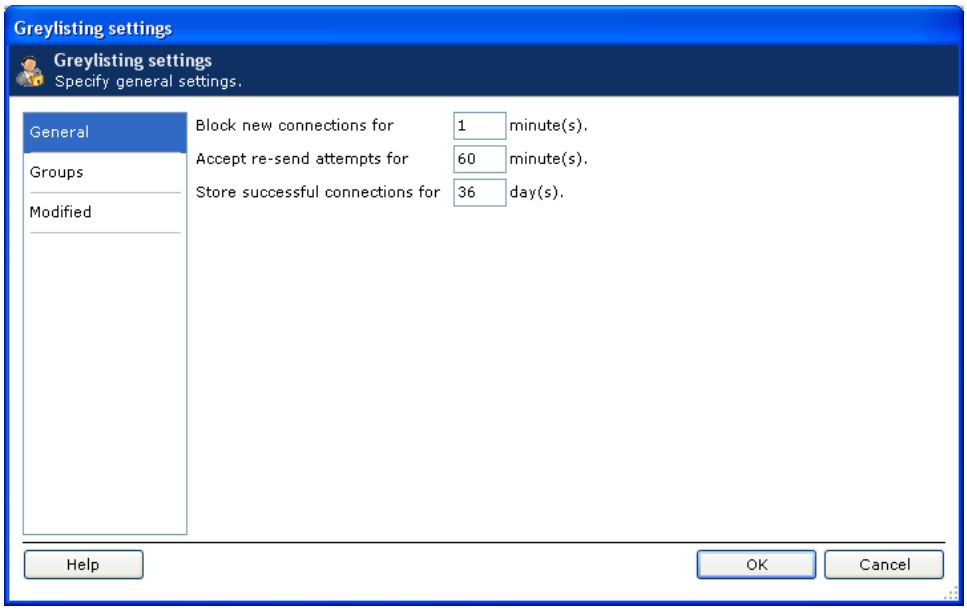
6.5 Greylisting

Info

Greylisting is a proven way to reduce spam messages and stop virus outbreaks. Most spammers use spamming applications that do not resend mails if they bounce, whereas legitimate mail servers automatically resend a message if it bounces. This means that by initially rejecting messages from new senders for approximately 2-3 minutes, legitimate emails will still be delivered and non-legitimate emails will not get through. Messages from senders on the Allow List will be delivered without any delays. This method can also be used to block virus outbreaks since virus infected machines typically use a non-intelligent SMTP agent that does not resend messages when they bounce.

To enable greylisting, follow the next steps:

1. Tick the option **Enable greylisting.**
2. Click on **Greylisting Settings** and go to the **General** tab. The following options are available:



Block new connections for x minute(s): Here you can specify for how many minutes Policy Patrol must block new connections. The default is one minute. This means that Policy Patrol will reject new connections for one minute. After the first minute it will accept any re-send attempts and add the sender connection to the Greylist Successful connections list. The message will still pass through the usual anti-spam checks before it is delivered to the recipient.

Note that if the X-Sender address is in the Allow List it will not be blocked by greylisting and will automatically be let through. However, if the X-Sender address is different from the From: address, and only the From: address is in the Allow List, then the message will be initially blocked by greylisting. This is because greylisting occurs before the actual message is received, when Policy Patrol only has access to the X-Sender address, not the From: address.

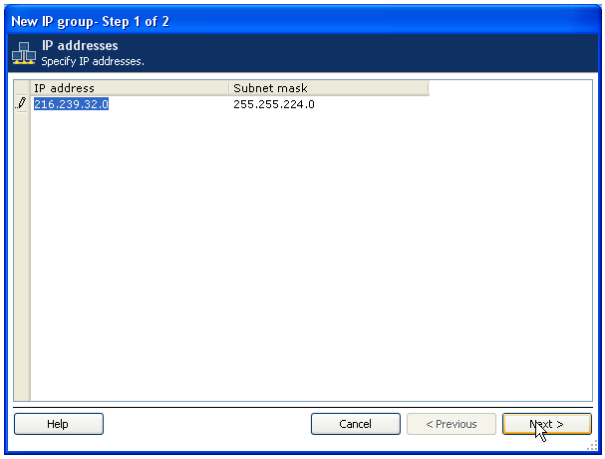
Accept re-send attempts for x minute(s): Here you can specify for how many minutes Policy Patrol must accept re-send attempts. The default setting is 60 minutes. This means that Policy Patrol will accept the message if it is resent within 60 minutes of the receipt of the initial message. If the resend attempt is sent more than 60 minutes after the first connection attempt, the attempt will be considered as a new connection.

Store successful connections for xx day(s): This setting specifies the number of days that successful connections must be stored. If a new connection is found to be in the successful connections list, it will be let through without any delay. The default for this setting is 36 days.

To view all connections in the database, select [All Connections] and click on the **Show** button. To view only pending connections, select **Pending connections** and click **Show**. To view only accepted connections, select **Accepted connections** and click **Show**. Rejected connections are deleted from the database.

3. Go to the **Groups** tab. This tab lists IP addresses that should be considered as a group, rather than an individual IP address. This can be useful when companies have many

different email servers and resend the message from different IP addresses. By entering these IP addresses as part of a group, a resend from any IP address in the group will allow the message to go through. Policy Patrol already includes a number of IP groups. To add more, click on **Add**. Enter the IP address and Subnet mask. Click **Next**. Enter the Group name and description and click **Finish**.



6.6 Bayesian Filtering

To use Bayesian filtering, check the box **Enable Bayesian filter spam protection**. You can select the threshold level ranging from very high to very low, where 'very high' means that a lower percentage of messages will be considered as spam and 'very low' means that a higher percentage of messages will be considered as spam. It is recommended however, to keep the level at **Normal**.

ⓘ Info

Bayesian filtering is a method for statistically analyzing message content and assigning a probability score to determine whether the mail is legitimate or non-legitimate. Policy Patrol uses this method to effectively identify and eliminate spam. Bayesian filtering is based on Bayes Theorem, a way of calculating the probability that an event will occur based on the number of times the event occurred in previous trials. Bayesian filtering makes use of two databases, one with legitimate mails and one with spam mails. When a new message arrives, Policy Patrol uses the Bayes Theorem to calculate the probability that the message is either legitimate or spam. The result is a probability score, where 0 is a legitimate message and 1 is a spam message. Most messages will include a probability score in between the two end values, for instance 0.939524 or 0.445324. The message with the score of 0.939524 is almost certainly spam, whereas the 0.445324 score indicates that the message is legitimate.

Select the threat classification to apply to messages detected as spam by Bayesian filtering by clicking on the button **Select threat classification**. By default the classification is set to 'Suspected spam'.

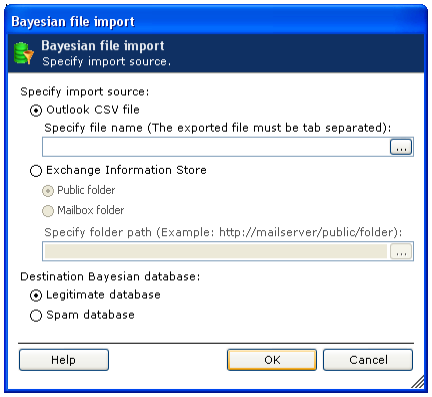
Before you start using Bayesian filtering, you must first fill the filter with approximately 1000 legitimate and 1000 spam messages. The Bayesian filter already includes the required number of spam messages. The easiest way to fill the database with legitimate messages is to check the box **Enable automatic Bayesian filter learning** in the Bayesian filter node. This will add all outgoing messages apart from DSNs and Out of office replies to the legitimate database. Policy Patrol will notify the Administrator by email when 1000 legitimate messages have been entered into the database. At this point, you can enable Bayesian filtering.

If you prefer to import messages instead of waiting for the Bayesian filter to auto learn from outgoing messages, consult the next paragraph on how to import messages.

6.6.1 Importing Messages into the Bayesian Database

Apart from auto learning from outgoing messages, messages can be manually imported into the Bayesian filter database in the following ways:

1. Import messages that have been exported from Microsoft Outlook: Click on the button  **Import messages**. Select **Outlook CSV File** as the import source. Now select the file with the exported messages from Outlook. The next step is to specify the destination database; select whether Policy Patrol should import the messages to the Legitimate or Spam database. Click **OK** to import the messages.



Note

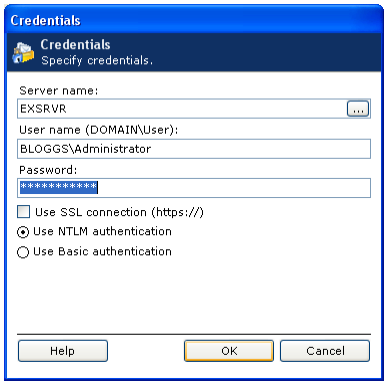
To export messages from Microsoft Outlook, go to Microsoft Outlook > **File** > **Import and Export**. Select **Export to a file** and click **Next**. Select **Tab separated Values (Windows)** and click **Next**. Select the folder to export the messages from and click **Next**. Enter the name for the exported file and click **Next**. Confirm the export and click **OK**.

2. Import messages from the Exchange Information Store: Click on the button  **Import messages**. Select the option **Exchange Information Store** and specify 'Public folder' or 'Mailbox folder' from where messages are to be imported from. Now specify the folder path or search for the folder by clicking on the **...** button. To be able to search for the folder you must enter the name of the Exchange Server and your credentials. Select

whether you wish to use NTLM authentication or Basic authentication. If you wish to use an SSL connection, tick the option **Use SSL connection (https://)**. Click **OK**.

Note

This option is not available in Policy Patrol for Exchange 2007/2010/2013.



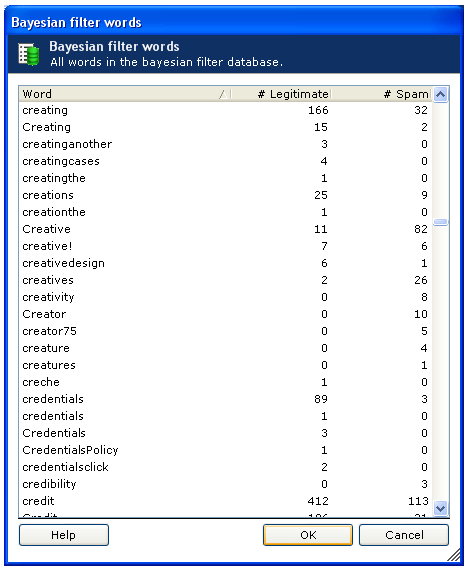
Now specify the destination database for the imported messages; select whether Policy Patrol should import the messages to the Legitimate or Spam database. Click **OK** to import the messages.

Tip

Once the legitimate and spam databases contain more than 1000 messages each, the Administrator will receive an email notification informing that Bayesian filtering can now be switched on.

6.6.2 Editing Words in the Bayesian Database

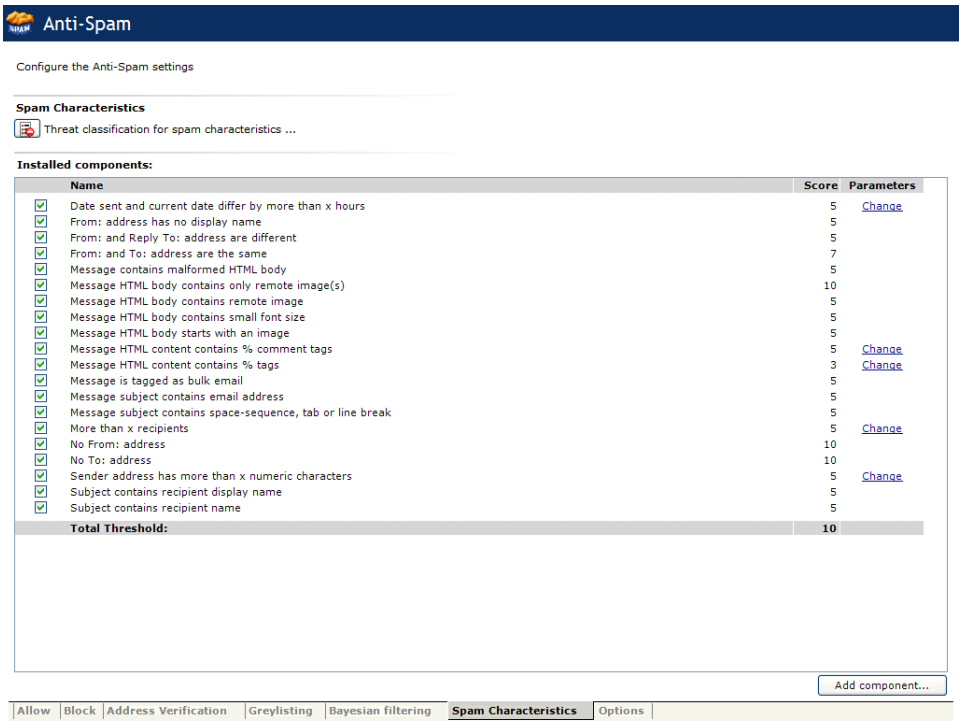
You can view and edit words in the Bayesian database by clicking on the button **View words**. It is advisable however not to make many changes since this might affect the effectiveness of the Bayesian filter. To delete a specific word, select the word and hit the [DELETE] key.



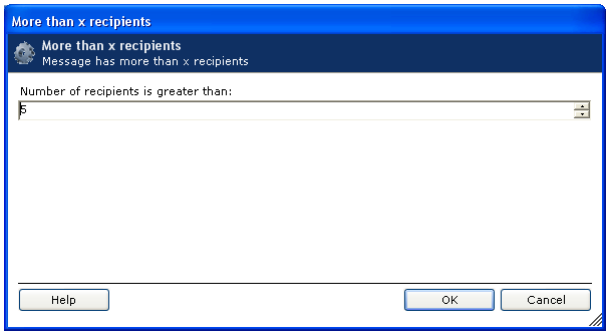
If you want to remove all the messages from the Bayesian filter databases and start again, you can do so by pressing the button **Delete all words**.

6.7 Spam Characteristics

Policy Patrol uses anti-spam components to check for common spam characteristics. Each anti-spam component checks for a specific spam characteristic and is given a score to count towards the total message threshold. Once the threshold is reached the message is considered as spam. Characteristics that surely indicate spam are given a higher score than more doubtful characteristics. By default Policy Patrol applies the appropriate score for each component. You only need to change the score if you want to fine tune the spam characteristics checking. You can do this by clicking in the score box for the appropriate spam characteristic. Similarly, the threshold can be changed by clicking in the **Total threshold** score box.



If the component includes a changeable parameter, you can change this by clicking on the Change link. For instance to change the number of recipients that should trigger the spam characteristic, click on the Change link next to **More than x recipients**. Adjust the number upwards or downwards and click **OK**.



If you do not want Policy Patrol to check for a certain spam characteristic, you can uncheck the box in order to disable it.

Click on **Threat classification for spam characteristics** and select the classification for messages that have reached the spam characteristics threshold. By default the classification is **Suspected spam**.

6.8 Options

6.8.1 Challenge/Response

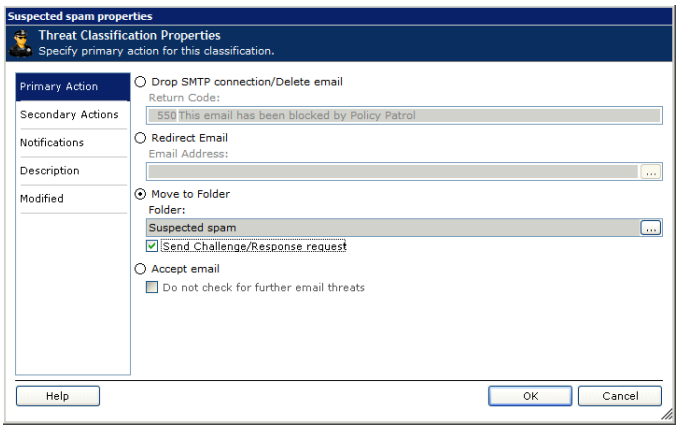
Policy Patrol allows you to configure challenge/response requests to be sent to all senders not in the allow list, or only when spam is already suspected.

ⓘ Info

Challenge/response is a system where you request new senders to verify their first message. After they have verified one message, the sender address is added to the Allow List and subsequent emails from this sender are automatically let through the filter. Since spammers use automated mail programs and are not able to verify all their spam messages, the challenge/response method is an effective method for filtering spam. The only drawback is that there is a possibility that legitimate senders will not bother to verify their emails. To circumvent this problem, you can configure Policy Patrol to only send the challenge/response email when you are not sure that the message is spam, but you do suspect that it might be spam. In other words you can configure the challenge/response request to be sent for the default Suspected spam classification.

If you want to send a challenge/response request to every new sender that is not in the allow list, you must select the option **Send challenge/response request to every sender not in allow list**. When a new sender sends an email, the message will be quarantined in the Challenge/response monitoring folder and an email message will be sent to the sender asking them to verify the message. As soon as the sender verifies the message, the sender will be added to the Allow List and the message will be delivered to the recipient. Any further email messages sent from this email address will automatically be let through. If the message is not verified within 3 days, the message is automatically deleted from the Challenge/response monitoring folder.

To configure Policy Patrol to only send challenge/response requests in certain instances, you must select the option **Only send Challenge/Response request when configured for threat**. If you are already certain that a message is spam there is no need to send a challenge/response request. Similarly if there is no reason to suspect spam, it might also not be necessary to send a challenge/response request. However if you suspect that a message is spam but are not 100% sure, it can be useful to send a challenge/response request for these messages only. In this case you would go to the **Email Threat Protection** node, in Threat Classifications double-click on the **Suspected spam** classification and in the **Primary action** tab select **Move to folder**, select the Challenge/response folder and tick the option **Send challenge/response request**.



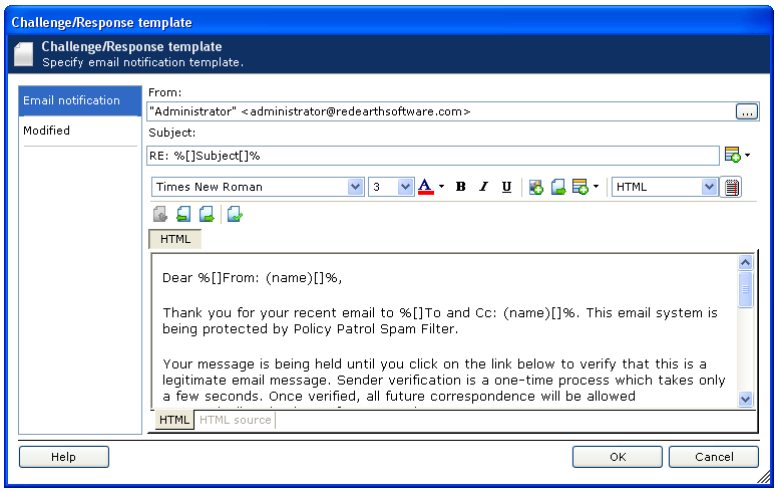
Note

Note that in order to use the challenge response feature, Internet Information Services (IIS) must be enabled on the Policy Patrol machine.

The link to your response page is automatically entered by the installation in 'Challenge/Response link'. This link is used by the sender to verify the email message and is included in the challenge/response email. The link should be listed as follows: http://<IPADDRESS>/ PolicyPatrolEmailCR/ where <IPADDRESS> is the external IP address of the Policy Patrol machine. For instance `http://100.255.25.34/PolicyPatrolEmailCR/`. Enter the From: address of the notification email in 'Send Challenge/Response request from'.

6.8.1.1 Editing the Challenge/Response Email

Policy Patrol includes a default challenge/response email message. If you wish to edit the message you can click on the button **Edit Challenge/Response template**. 



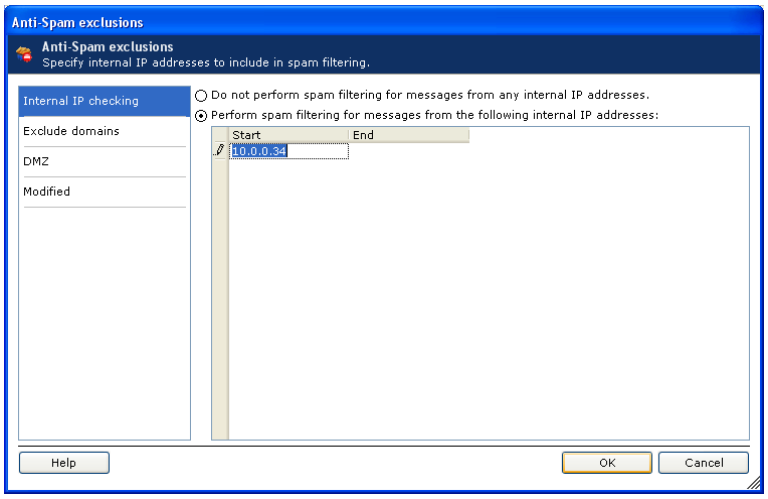
You will be able to specify the From: email address and the subject of the message. For more information on how to configure the challenge/response template, consult the chapter 'Creating Templates'.

6.8.2 Anti-Spam Exclusions

Sometimes you need to exclude certain IP addresses from spam filtering. These can be configured in Exclusions.

6.8.2.1 Internal IP Checking

By default Policy Patrol will not check any messages for spam if they are sent from a local IP address, assuming that emails being sent from your own server are not spam. However, if you have a mail server that is forwarding mail to Policy Patrol from an internal IP address (for instance from a frontend server or bridgehead server), you must select **Perform spam filtering for messages from the following internal IP addresses**, and enter the IP address in this list, in order for Policy Patrol to perform spam filtering.



Note

You do not have to enter the mail server IP address if Policy Patrol is installed on a separate machine. This is because Policy Patrol will receive the mail directly from the Internet, not from the mail server.

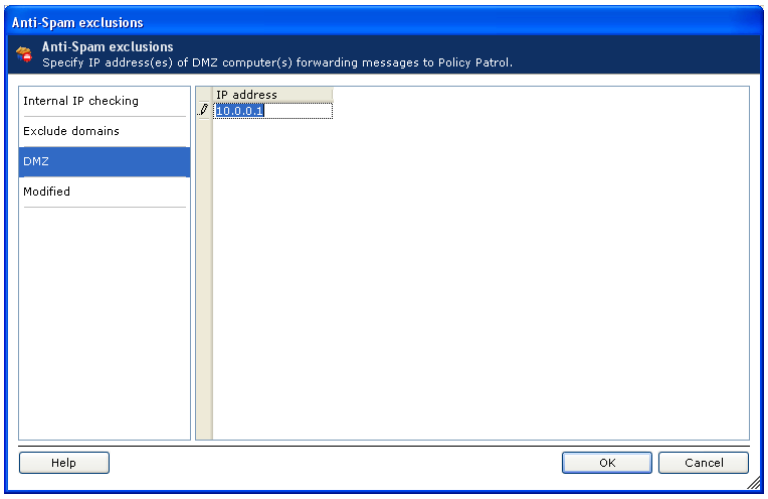
6.8.2.2 Exclude Domains

If you have recipient verification enabled and there are users who are remotely using Outlook Express and sending out mail via your mail server, Policy Patrol will reject the message since the message is seen as incoming and the recipient will not be found in the lookup list. For example if user@bloggs.com sends a mail via Outlook Express to user@externaldomain.com, Policy Patrol will block this message since it is seen as an externally received message with no valid internal recipient. Therefore you must exclude the emails sent from remote Outlook Express users by entering their helo/ehlo domain in this list. The helo/ehlo domain can be found in the SMTP logs

located in C:\WINDOWS\system32\Logfiles. In the file, search for the user(s) and it will display the helo name that you need to add in this tab.

6.8.2.3 DMZ

If you have a DMZ you can enter the IP address of the DMZ machine in this list. This means that Policy Patrol will not look up the IP address of the DMZ machine in the DNS block lists and will only check the headers for domains on the DNS Block lists. In this way you will prevent unnecessary lookups every time the DMZ forwards a message to the Policy Patrol machine.



6.9 Forwarding Spam to the Users' Junk Mail Folders

If you want to forward spam to the users' junk mail folders, you must follow the instructions below depending on the Exchange Server version that you have installed.

6.9.1 If You Have Exchange 2007/2010/2013

To forward spam mails to the user's junk mail folder with Exchange 2007/2010/2013, you must configure Policy Patrol to add an SCL value to the message (in secondary actions of the threat classification). Then you must configure Exchange Server to forward the messages that reach the SCL value to the user's junk mail folder. For more information on how to do this, please consult the following Microsoft TechNet article: http://technet.microsoft.com/en-us/library/aa995744.aspx.

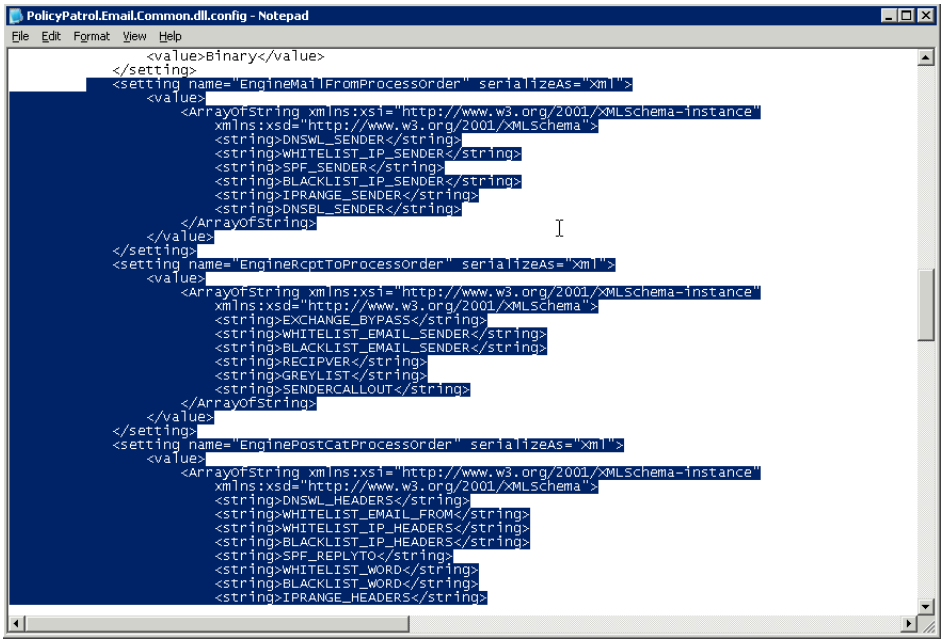
6.9.2 Disabling Anti-spam

If you do not want Policy Patrol to check for spam, you can disable Anti-spam checking by going to the Email Threat Protection node and unchecking the option **Anti-spam**.

6.10 Changing the Order of Spam Checking Modules

To change the default order in which Policy Patrol processes spam checks, browse to the Policy Patrol Email directory, by default in C:\Program Files\Red Earth Software\Policy Patrol Email (32-

bit) or C:\Program Files (x86)\Red Earth Software\Policy Patrol Email (64-bit) and open the file **PolicyPatrol.Email.Common.dll.config** in Notepad. Note: Make a backup of this file before you make any edits so that you can always revert to the original version.



Browse to the following entries:

```
<setting name="EngineMailFromProcessOrder" serializeAs="Xml">
        <value>
          <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema">
            <string>DNSWL_SENDER</string>
            <string>WHITELIST_IP_SENDER</string>
            <string>SPF_SENDER</string>
            <string>BLACKLIST_IP_SENDER</string>
            <string>IPRANGE_SENDER</string>
            <string>DNSBL_SENDER</string>
          </ArrayOfString>
        </value>
      </setting>

      <setting name="EngineRcptToProcessOrder" serializeAs="Xml">
        <value>
          <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema">
            <string>EXCHANGE_BYPASS</string>
            <string>WHITELIST_EMAIL_SENDER</string>
            <string>BLACKLIST_EMAIL_SENDER</string>
            <string>RECIPVER</string>
            <string>GREYLIST</string>
            <string>SENDERCALLOUT</string>
          </ArrayOfString>
```

```
    </value>
  </setting>

  <setting name="EnginePostCatProcessOrder" serializeAs="Xml">
    <value>
      <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <string>DNSWL_HEADERS</string>
        <string>WHITELIST_EMAIL_FROM</string>
        <string>WHITELIST_IP_HEADERS</string>
        <string>BLACKLIST_IP_HEADERS</string>
        <string>SPF_REPLYTO</string>
        <string>WHITELIST_WORD</string>
        <string>BLACKLIST_WORD</string>
        <string>IPRANGE_HEADERS</string>
        <string>DNSBL_HEADERS</string>
        <string>SURBL</string>
        <string>SPAMCHAR_LANGUAGES</string>
        <string>SPAMCHAR_COMPONENTS</string>
        <string>GEOIP_BLOCK</string>
        <string>BAYESIAN</string>
        <string>CR_ALL</string>
      </ArrayOfString>
    </value>
  </setting>
```

The following three lists are available for the ordering of anti-spam modules:

Setting	Description
EngineMailFromProcessOrder	This setting contains the order of spam checks that are performed after the MAIL FROM command. The order of this list can be change freely, for example, moving DNSBL_SENDER to the top of the list would cause Policy Patrol to first do a DNSBL lookup, before checking the IP allow list.
EngineRcptToProcessOrder	The order of spam checks that are performed after each RCPT TO command. If user-based allow list/block list is not used, WHITELIST_EMAIL_SENDER and BLACKLIST_EMAIL_SENDER can be moved to the EngineMailFromProcessOrder list.
EnginePostCatProcessOrder	The order of spam checks that are performed after the message is received.

To change the order of spam checking you can simply move the order of the strings within the lists. For instance if you wish Bayesian filtering to be checked before country blocking

(GEOIP_Block), you can modify the entry to be as follows:

```
<ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema">
               <string>DNSWL_HEADERS</string>
               <string>WHITELIST_EMAIL_FROM</string>
               <string>WHITELIST_IP_HEADERS</string>
               <string>BLACKLIST_IP_HEADERS</string>
               <string>SPF_REPLYTO</string>
               <string>WHITELIST_WORD</string>
               <string>BLACKLIST_WORD</string>
               <string>IPRANGE_HEADERS</string>
               <string>DNSBL_HEADERS</string>
               <string>SURBL</string>
               <string>SPAMCHAR_LANGUAGES</string>
               <string>SPAMCHAR_COMPONENTS</string>
               <string>BAYESIAN</string>
               <string>GEOIP_BLOCK</string>
               <string>CR_ALL</string>
            </ArrayOfString>
         </value>
      </setting>
```

In addition, some of these anti-spam checks can be moved between the three lists. However not all of them can be moved. For example: WHITELIST_IP_SENDER can be moved to ' EngineRcptToProcessOrder' or 'EnginePostCatProcessOrder', whereas 'WHITELIST_EMAIL_FROM' cannot be moved to any other list and must exist in 'EnginePostCatProcessOrder'. Any anti-spam actions that check headers or email content must be in the 'EnginePostCatProcessOrder' list. This is because these anti-spam checks can only be performed after the email message has been received. If an anti-spam component is moved to a list where it is not supported, an error will be visible in the message history details for messages on which Policy Patrol tried to run the anti-spam.

Note that if you remove entries Policy Patrol will skip that anti-spam check.

Below is a list of the different strings that are available along with a description:

String	Description
WHITELIST_IP_SENDER	Sender IP allow list
SPF_SENDER	Sender SPF
BLACKLIST_IP_SENDER	Sender IP block list
IPRANGE_SENDER	Sender IP ranges
DNSBL_SENDER	Sender IP DNSBL
EXCHANGE_BYPASS	Exchange bypass (Sender ID, Safe Sender list
WHITELIST_EMAIL_SENDER	Sender email allow list
BLACKLIST_EMAIL_SENDER	Sender email block list
RECIPVER	Recipient verification
GREYLIST	Greylist checking
SENDERCALLOUT	MX record verification, SMTP callout
WHITELIST_EMAIL_FROM	From: email allow list

WHITELIST_IP_HEADERS	Header IP(s) allow list
BLACKLIST_IP_HEADERS	Header IP(s) block list
SPF_REPLYTO	Reply-To SPF
WHITELIST_WORD	Word/phrase allow list
BLACKLIST_WORD	Word/phrase block list
IPRANGE_HEADERS	Header IP(s) ranges
DNSBL_HEADERS	Header IP(s) DNSBL
SURBL	SURBL
SPAMCHAR_LANGUAGES	Language/Character set blocking
SPAMCHAR_COMPONENTS	Anti-Spam components
GEOIP_BLOCK	Country blocking policies
BAYESIAN	Bayesian filtering
CR_ALL	Challenge/Response (all messages from senders not on the allow list)

Chapter 7

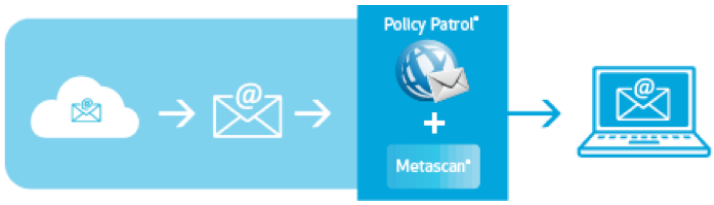
Anti-Malware

Policy Patrol can check email messages for viruses using Metascan multi anti-malware scanner. This chapter explains the different anti-virus settings that can be configured.

7.1 Metascan Multi AV Scanner

No antivirus engine is perfect. With over 450,000 new threats emerging daily, it would be impossible for any single antivirus product to provide guaranteed detection 100% of the time.

Using Metascan technology, Policy Patrol can quickly scan email attachments with multiple anti-malware engines to detect and block advanced threats. By using multiple anti-malware engines, Metascan increases detection rates for all types of malware without the hassle of licensing and maintaining multiple antivirus engines. Metascan can also perform file sanitization and file type checking, preventing zero-day and targeted attacks.



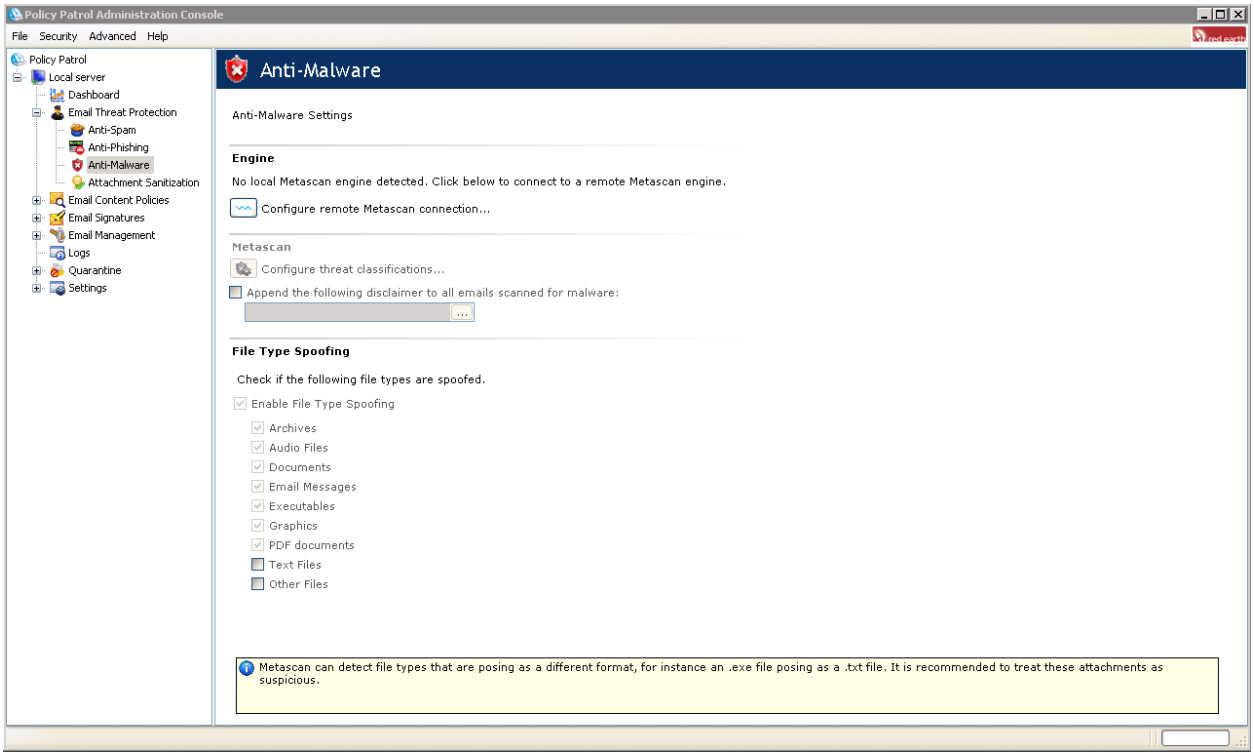
7.2 Metascan Online and On-Premise

Metascan can be purchased as an add-on for Policy Patrol. Metascan is available as an on-premise solution and as a cloud solution. The on-premise solution is available in packages between 4-30 anti-malware engines. More information about the different packages can be found on this page: http://www.policypatrol.com/metascan-advanced-threat-prevention.

Metascan Online is a cloud-based deployment of Metascan. With Metascan Online, Policy Patrol will scan your email attachments with 40+ anti-malware engines. New in version 10: OPSWAT is providing a free Metascan Online subscription to Policy Patrol users up to the free edition scan limits. Request your free Metascan Online subscription from the following page: http://www.policypatrol.com/request-free-metascan-online. Licenses for increased scan limits are available for purchase.

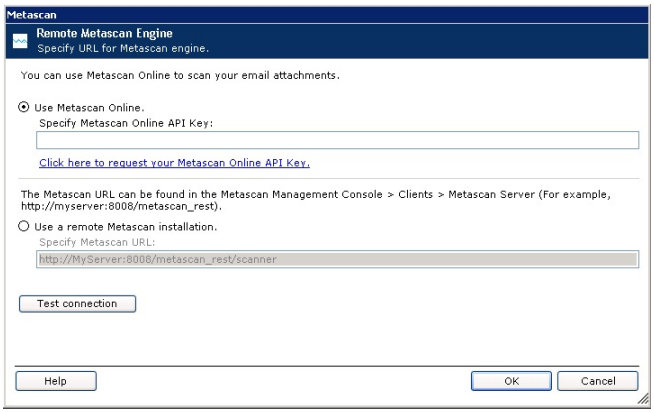
7.3 Metascan Online

Metascan Online can be used to scan email attachments for viruses with 40+ anti-malware engines. To configure Metascan Online go to **Email Threat Protection** > **Anti-Malware**. Click on **Configure remote Metascan connection**.



Enable the option **Use Metascan Online** and enter your Metascan online API key.

New in version 10: OPSWAT is providing a free Metascan Online subscription to Policy Patrol users up to the free edition scan limits. Request your free Metascan Online subscription from the following page: http://www.policypatrol.com/request-free-metascan-online. Licenses for increased scan limits are available for purchase from OPSWAT.



Note: If you have Metascan On-Premise installed on the same machine as Policy Patrol, you still not see the Metascan Online configuration options. Note that file sanitization and file type verification is only offered with Metascan On-Premise, not Metascan Online.

7.4 Metascan On-Premise

In order to use Metascan On-Premise with Policy Patrol, you need to install Metascan on your network. Metascan can be installed on the same machine as Policy Patrol, but it can also be installed on a separate machine. If Metascan is installed on a separate machine, you must configure Policy Patrol to connect to the Metascan server.

Note: Attachment sanitization is only available if you install Metascan on the same machine as Policy Patrol.

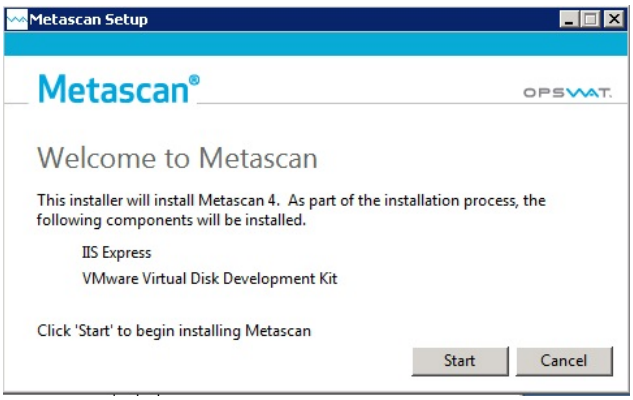
7.5 Installing Metascan

To obtain your trial version of Metascan on-premise, go to http://www.policypatrol.com/policy-patrol-mail-security/download-metascan/.

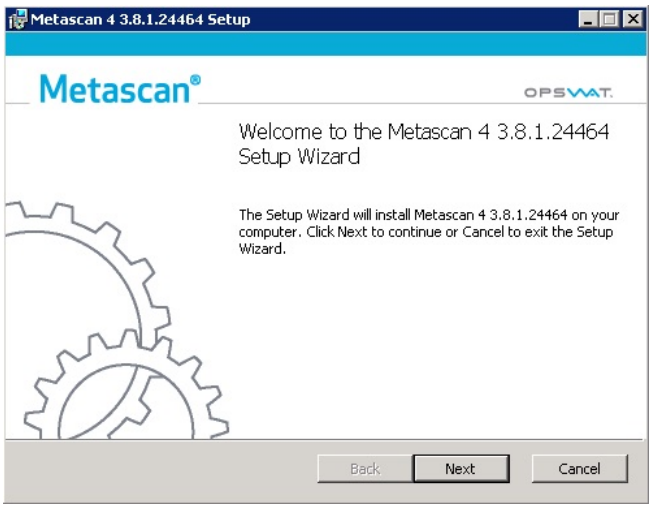
Once you have downloaded Metascan, follow the next steps:

Note that Metascan requires .NET Framework 4.0 or later to be installed on the system.

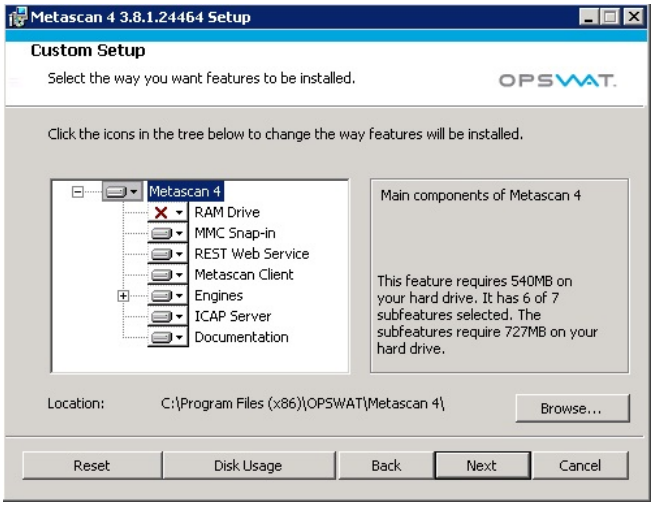
1. Double-click on the executable. The welcome screen will appear. Click on **Start** and wait until the Metascan prerequisites are installed.



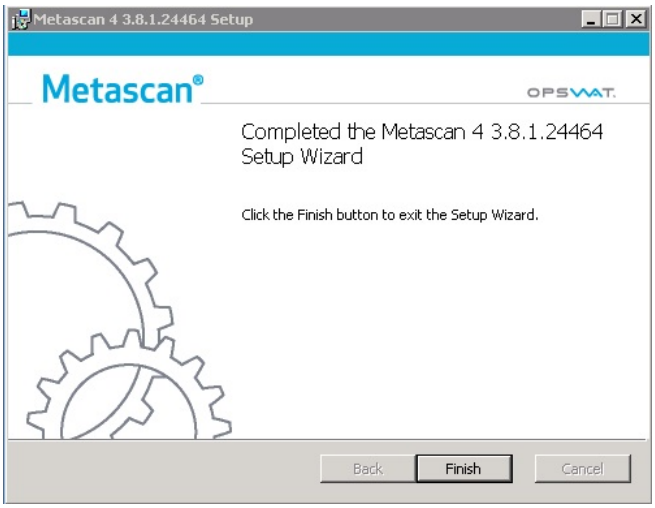
2. When the Setup Wizard appears, click **Next**.



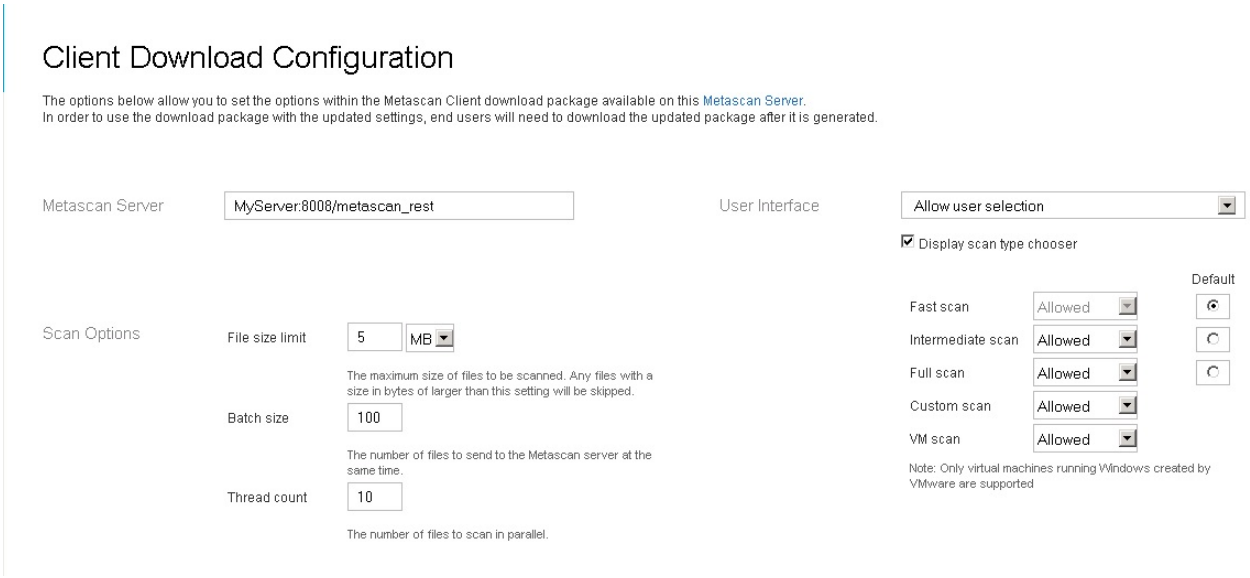
3. Select **Accept the terms in the License Agreement** and click **Next.**
4. Choose which components of Metascan you would like to install.



5. Click **Next.**
6. Click **Install**.



7. Click **Finish** to complete the installation.
8. Go to **Start** > **OPSWAT** > **Metascan Management Console**. The console will open in a browser. You can configure scanning options from **Workflow** in the top menu.
9. If you installed Metascan on a different machine than Policy Patrol: Go to **Clients** in the top menu.



- Copy the link from the **Metascan Server** box for entering in Policy Patrol (see below).
- Make sure you open the port specified in the URL in order to allow Policy Patrol to remotely connect to this server (in the screen above this is port 8008).

Tip

Metascan clients are also available for the Metascan server, allowing you to scan endpoint systems for advanced threats.

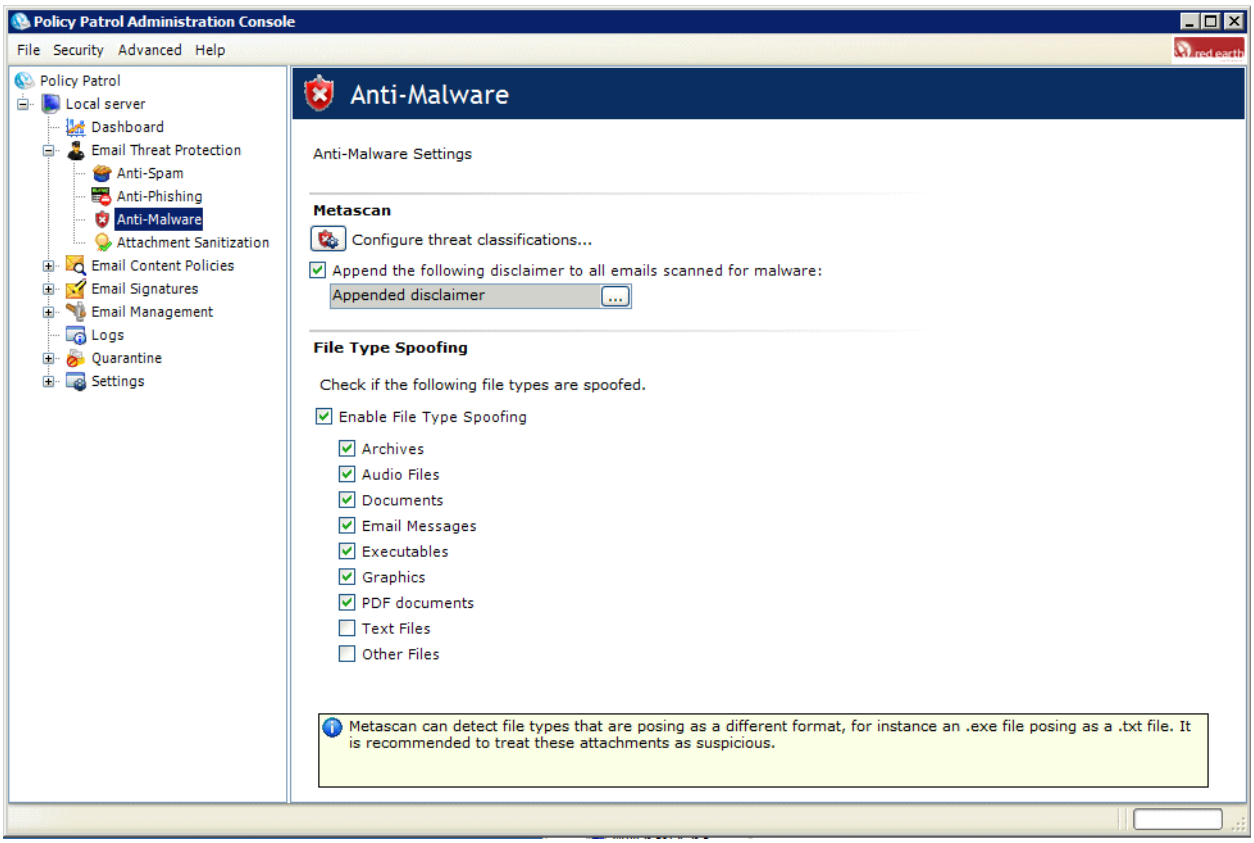
7.6 Enabling Metascan in Policy Patrol

After installing Metascan, you must enable Metascan in Policy Patrol. Follow the instructions below depending on whether you have installed Metascan on the same machine as Policy Patrol or on a separate machine.

7.6.1 If Metascan is Installed on the Same Machine as Policy Patrol

If you installed Metascan after Policy Patrol Email was installed, restart the Policy Patrol Email Server service for it to detect that Metascan is available.

If Metascan is installed on the same machine as Policy Patrol you can enable Metascan multi anti-virus scanning by going to the **Email Threat Protection** node and checking the **Anti-Malware** box.



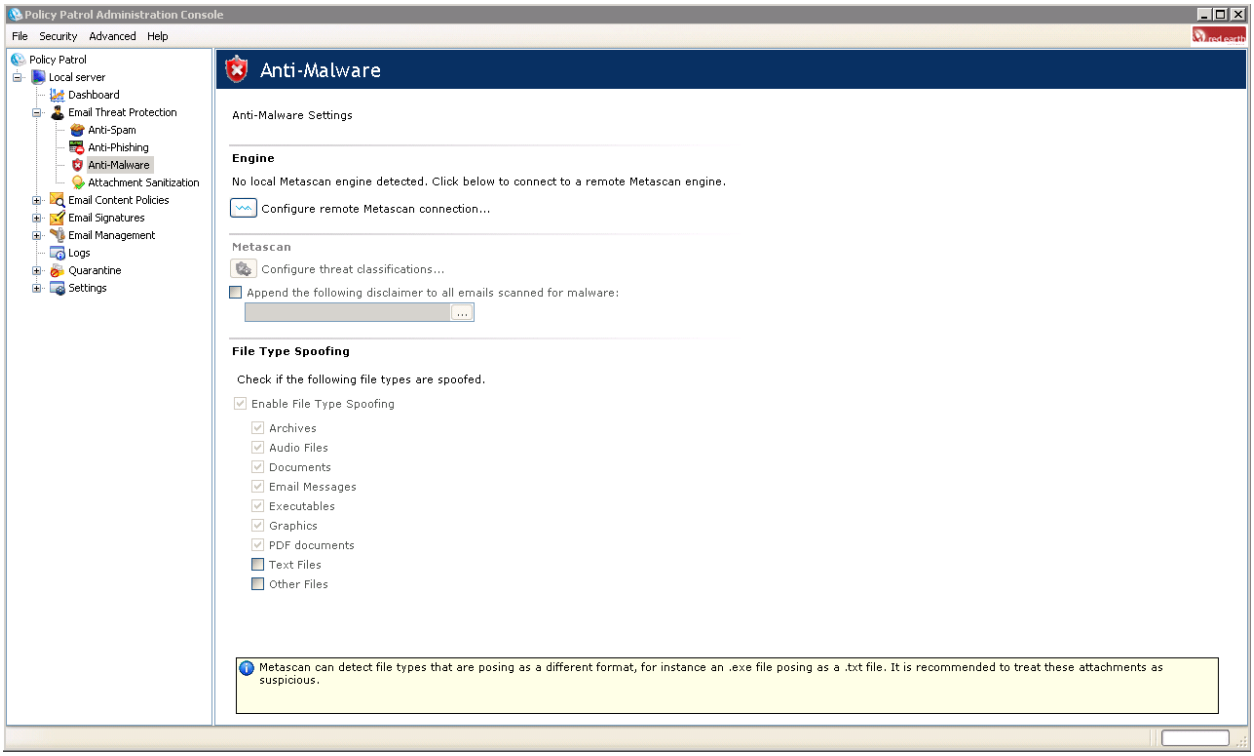
In **Configure threat classifications..** you can select what actions to take on each message that has been detected as containing a known or possible virus. Policy Patrol includes the following malware threat classifications: Infected, Suspicious, Password protected and Spoofed file types. The available options for each classification are discussed in paragraph 5.2 'Threat Classifications'.

7.6.2 If Metascan is Installed on a Separate Machine

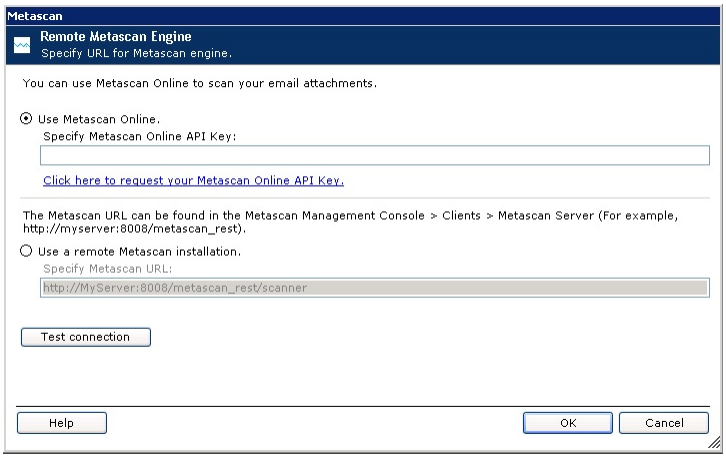
If you installed Metascan after Policy Patrol Email was installed, restart the Policy Patrol Email Server service for it to detect that Metascan is available.

If Metascan is installed on a different machine than Policy Patrol, you can enable Metascan multi anti-virus scanning by following the next steps:

1. Go to **Anti-Malware** and select the option **Configure remote Metascan connection**.



2. Specify the URL of the machine where Metascan is installed. This URL can be found in the **Metascan Management Console** > **Clients** > **Metascan Server**. Make sure that the port in the URL is open (in this example it is port 8008).



3. Click **Test connection**. A message box will appear saying that the connection was successfully created. Click **OK**.

4. Now enable Metascan by going to the **Email Threat Protection** node and checking the **Anti-Malware** box.

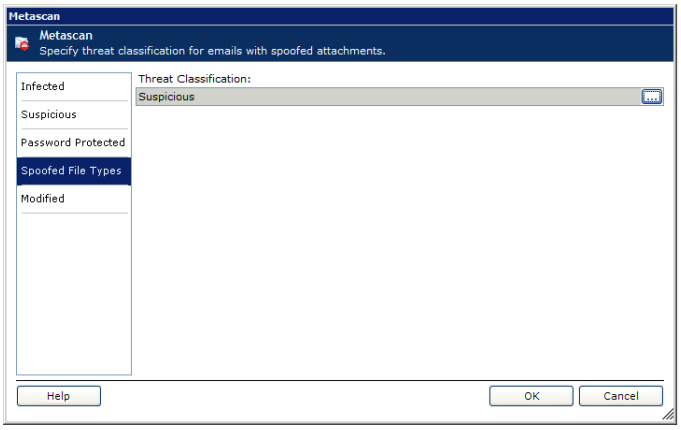
In **Configure threat classifications..** you can select what actions to take on each message that has been detected as containing a known or possible virus. Policy Patrol includes the following malware threat classifications: Infected, Suspicious, Password protected and Spoofed file types. The available options for each classification are discussed in paragraph 5.2 'Threat Classifications'.

7.7 Adding a Disclaimer

If you want to add a footnote to messages that have been scanned for viruses, select the option **Append the following disclaimer to all messages scanned for viruses** and click on the **...** button to select the Disclaimer template. For instance, you could add the line 'This message was scanned for viruses by Policy Patrol'.

7.8 File Type Spoofing

In addition to anti-malware scanning, Metascan can verify and detect spoofed email attachment types, preventing for instance .exe files posing as .txt files from entering your organization.



In the list, select which file types need to be verified for file type spoofing. If Metascan determines that a file is spoofed, Policy Patrol will take the actions as specified in the selected Threat Classification. To view the configured actions, click on the Browse button next to the threat classification, right-click the threat classification in the list and select **Edit**. The available options are discussed in paragraph 5.2 Threat Classification.

Note that Attachment Sanitization options are described in paragraph 5.6.

Chapter 8

Email Content Policies

Policy Patrol includes a powerful policy wizard that allows you to specify users, conditions, exceptions and actions. This chapter describes how to configure your Email security policies in Policy Patrol.

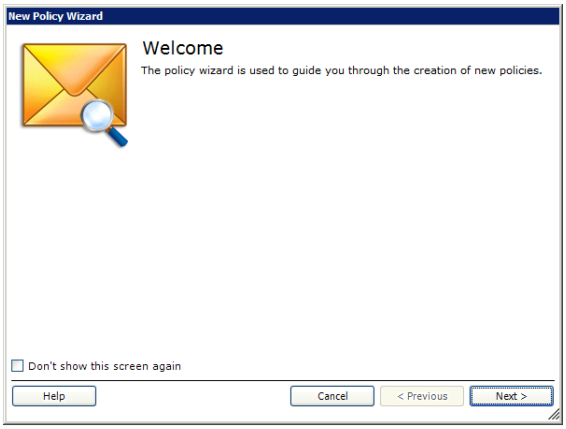
8.1 Configuring an Email Content Policy

To configure a new Email Content Policy, go to **Email Content Policies**, select the appropriate folder and click **New...**. If you wish to create a new folder, right-click on **Email Content Policies** and select **New folder...** In the folder click on the **New...** button.

Note

Remember that you must first select a folder before you can create a new policy.

The Policy wizard will appear. In the Welcome screen, click **Next.**



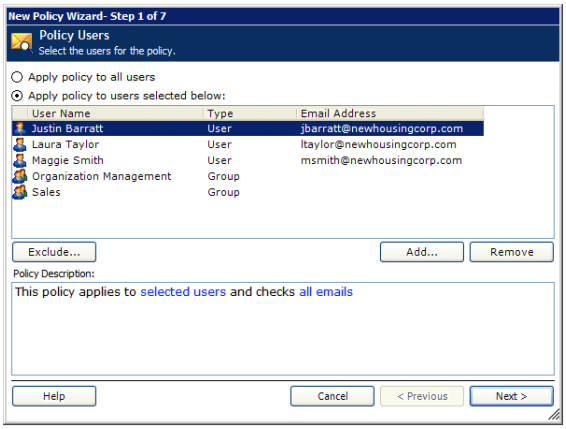
The policy wizard will now guide you through the different steps described below.

? Info

From step 2 onwards. the wizard is divided into two panes. The policy options are displayed in the top pane and the policy description in the bottom 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 for a selected option, a dialog will pop up asking you to specify further options. Once a value is set, the link color will appear in blue in the bottom pane. If you do not select a value, the link will appear in red since it still needs to be configured. If you have not yet set all values when you click finish to create your policy, a warning will pop up. You will still be able to create the policy, but the policy will not be enabled until you set all values.

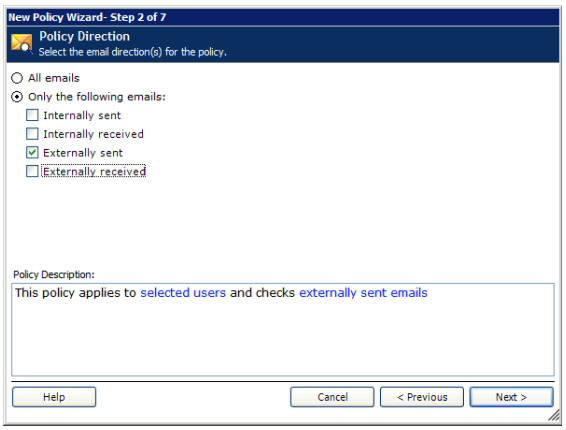
8.1.1 Step 1. Policy Users

To apply the policy globally, select **Apply policy to all users**. To apply the policy to certain users, groups, or domains select **Apply policy to users listed below** and click **Add...** Select the users for the policy. To select multiple users, hold down the [CTRL] or [SHIFT] keys or use the **Select all** button. When you have selected the users for the policy, click **OK**. To remove users from the policy, select the user(s) and click **Remove**. If you wish to add exceptions, for instance if you wish the policy to apply to all users apart from the Board of Directors, click on **Exclude...** and **Add...**. Select the user(s) to exclude, click **OK** and **Close**. Click **Next**.



8.1.2 Step 2. Policy Direction

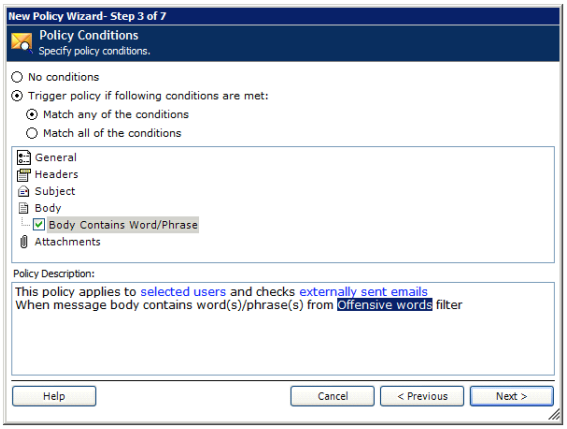
Specify whether you wish to apply the policy to all messages or only internally sent and/or received messages, and/or externally sent and/or received messages. Remember that Policy Patrol can only apply policies to internal messages if you have installed Policy Patrol on an Exchange Server machine. Click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



8.1.3 Step 3. Policy Conditions

Here you must specify which conditions should be met for the policy to trigger. If the policy should always trigger, leave **No conditions** selected and click **Next**. If the policy should only trigger in certain circumstances, select **Trigger policy if following conditions are met**. The different conditions are sorted into the following threat classifications: General, Headers, Subject, Body and Attachments.

If any of the conditions must be met, select **Match any of the conditions**. For instance, if you want to create a policy that deletes messages that contain certain words or are from a specified sender, 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.



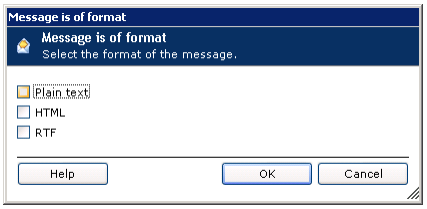
Available conditions:

- **General**

  ☑ **Message is encrypted**: This condition checks whether a message is encrypted.

  ☑ **Message is digitally signed**: This condition checks whether a message is digitally signed.

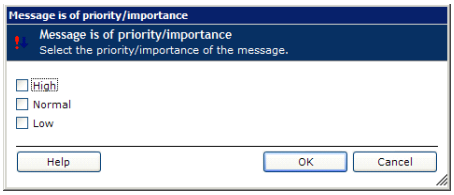
☑ **Message is of format**: Specify whether the message should be of plain text, HTML and/or rich text format.



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.

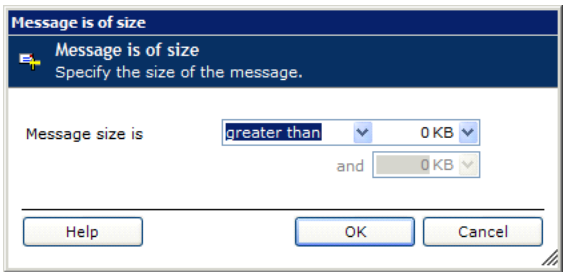
☑ **Message is of priority/importance**: Specify whether the message should be of High, Normal and/or Low priority.



☑ **Message is of sensitivity**: Specify whether the message should be Normal, Personal, Private and/or Confidential.



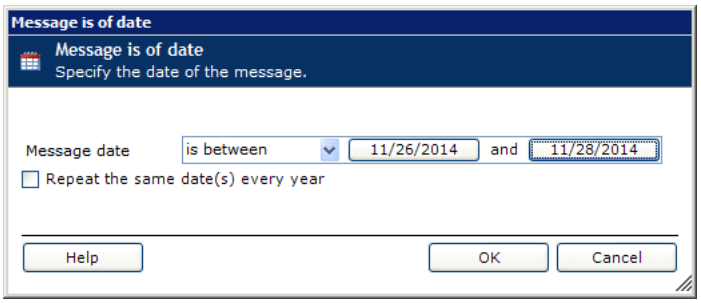
☑ **Message is of size**: Specify whether the message size (this includes headers, message text and attachments) should be greater than, less than, between or not between certain values. If you select **greater than** or **less than**, the value you enter will not be included, e.g. if you select greater than 1 MB, the policy 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 policy 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 policy will not trigger for messages of 2 MB and 3 MB and any size in between.



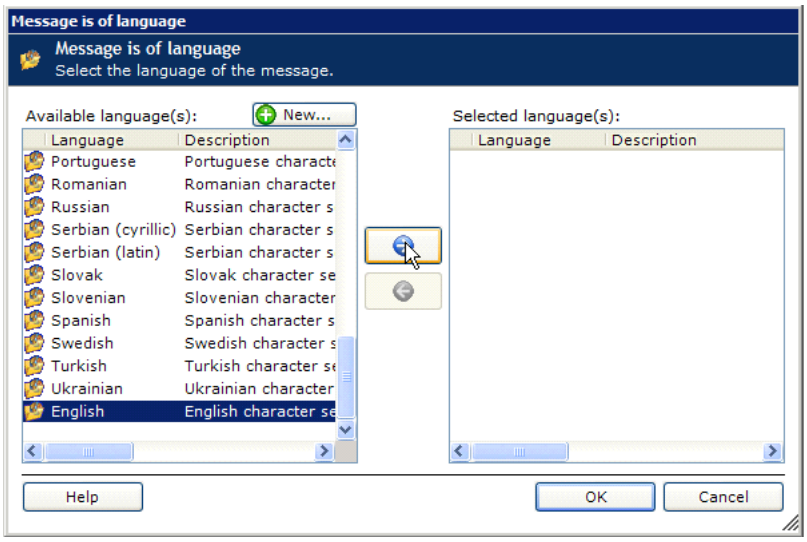
Note

Policy Patrol counts the actual message size as received by the mail server. This can be 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 **equals**, the policy will only trigger on the selected date. If you select **is before** or **is after**, the policy will trigger before or after the selected date (date itself will not be included). For instance, if you specify that a policy should trigger for dates before October 1st, the policy will trigger for messages sent on or before September 30th, but not on October 1st. If you select **between** or **not between**, this will include the two values. For instance, if you select **between** 5th and 7th September, the policy will trigger for messages sent on 5th, 6th and 7th September. If you select **not between** 5th and 7th September, the policy will not trigger for messages sent on 5th, 6th and 7th September. Check the option **Repeat the same date(s) every year** if you wish the policy to trigger on the specified days of the month, irrespective of the year.



☑ **Message is of language**: Specify whether the message should use a certain language. Select the language in the left pane and clicking the ➔ button. To edit a configured language, right-click the language and select **Edit**. To create a new language, click on the **New** button. When you are done, click **OK**. Languages can be configured in **Settings** > **Languages**.



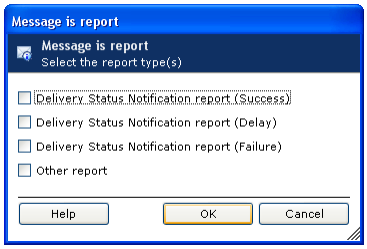
☑ **Message contains read receipt request**: By checking this option Policy Patrol will check if the message contains a read receipt request. There are no further options for this condition.

☑ **Message 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.

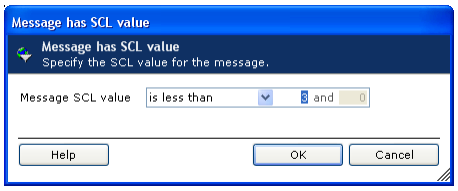
☑ **Message is DSN report**: Specify whether the message should be a Success, Delay, Failure notification, or Other report (report without status code).

Note

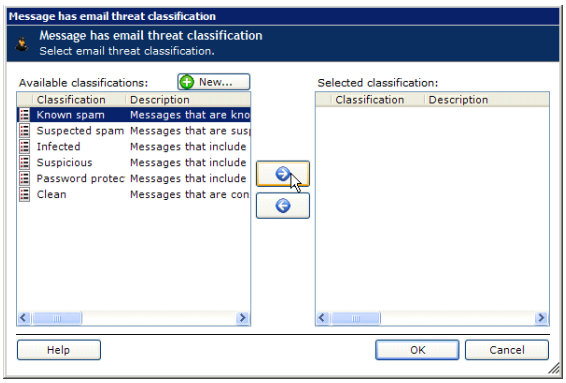
If you wish to filter Delivery Status Notifications (DSNs), you must select to check externally sent and/or internally sent messages in step 2 of the Policy Wizard.



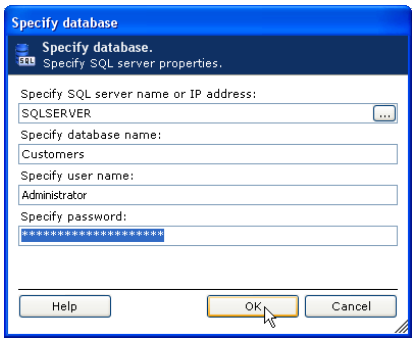
☑ **Message has SCL value:** By checking this option Policy Patrol will check to see if the message has an SCL value within the specified range. The SCL value can be from 0-9, with 0 indicating a legitimate message and 9 indicating a spam message. The negative value -1 can also be used, this indicates that the message should be allowed through.



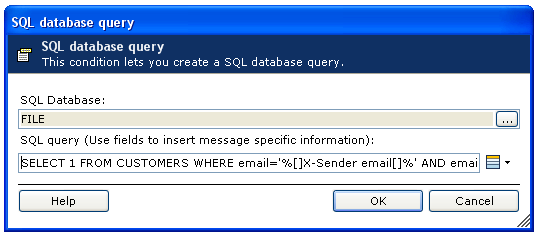
☑ **Message has email threat classification:** This condition allows you to apply policies to messages that have been classified by certain threat classifications. If you only want to handle spam using the Email Content Policies (for instance if you want to handle spam differently per user), you can configure the action **Accept message** in the threat classification and select this condition to trigger the appropriate policy.



☑ **Message matches SQL database query:** This condition allows you to look up information in a SQL database and search for this information in any message or user field. For instance you could use this condition to trigger a policy only when senders or recipients are found in the database. Firstly you need to specify the SQL database settings by clicking on …



Enter the SQL Server name or IP address, or click on **...** to browse to the machine. Enter the database name and enter the user name and password for accessing the database. Click **OK**.



Now you must enter the SQL query in the following format:

SELECT 1 FROM [SQL_table_name] WHERE [column_name]=%[]Message field[]%

Where:

[SQL_table_name] = name of the table in SQL Server to look up information from

[column_name] = name of the table column where you want to look up information

%[]Message field[]% = Message field that you want to match in the SQL table column

For instance, you have a SQL table called CUSTOMERS and in the 'Email' column you have listed all your customers' email addresses. To trigger a policy that applies only to emails sent to email addresses in the CUSTOMERS table, excluding those entries in the database without an email address, you must enter the following query:

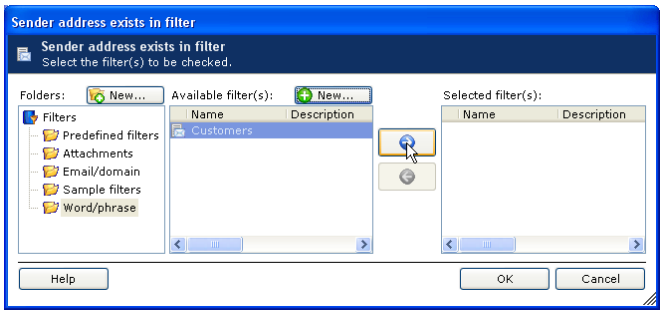
```
SELECT 1 FROM CUSTOMERS WHERE Email='%[]X-Receiver email[]%' AND email <> ''
```

☑ **Message is from country:** Select this option if you wish to apply policies to emails from certain countries. Select the countries in the left column and click on the right arrow button. When you are done, click **OK**.



- **Headers**

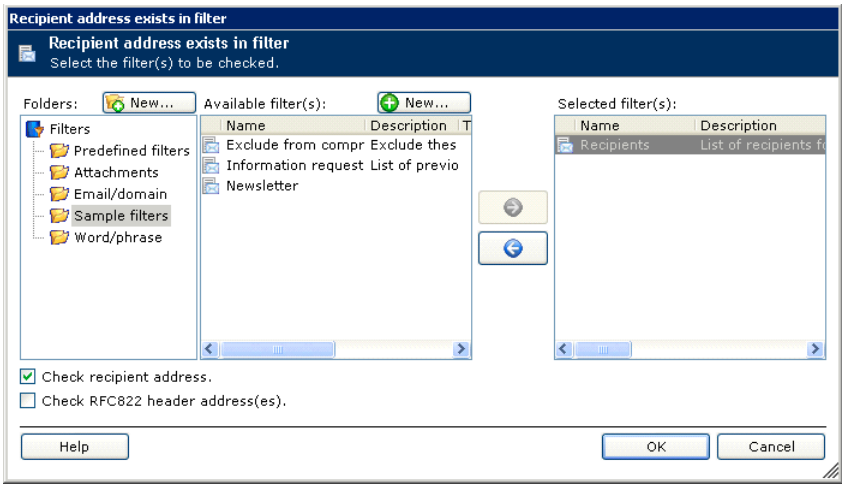
☑ **Sender address exists in filter**: Select the Email/domain filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol will check the From: and X-Sender fields for the configured address(es).



Note

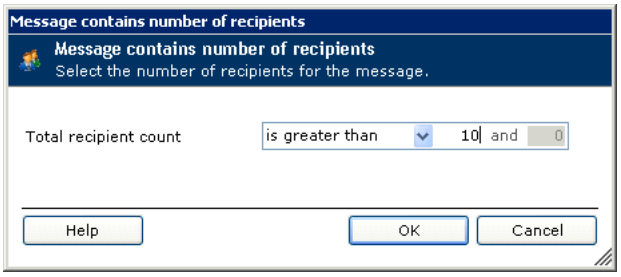
The predefined filters folder contains the Email block list and Email allow list filter. These lists are configured from Anti-spam > Allow/Block. If you wish to handle spam messages via the policies you can select these filters if you wish.

☑ **Recipient address exists in filter**: Select the Email/domain filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. If you wish Policy Patrol to check the X-Receiver field, select the option **Check recipient address**. If you wish to check the To: and Cc: fields, enable the option **Check RFC822 header address(es)**.

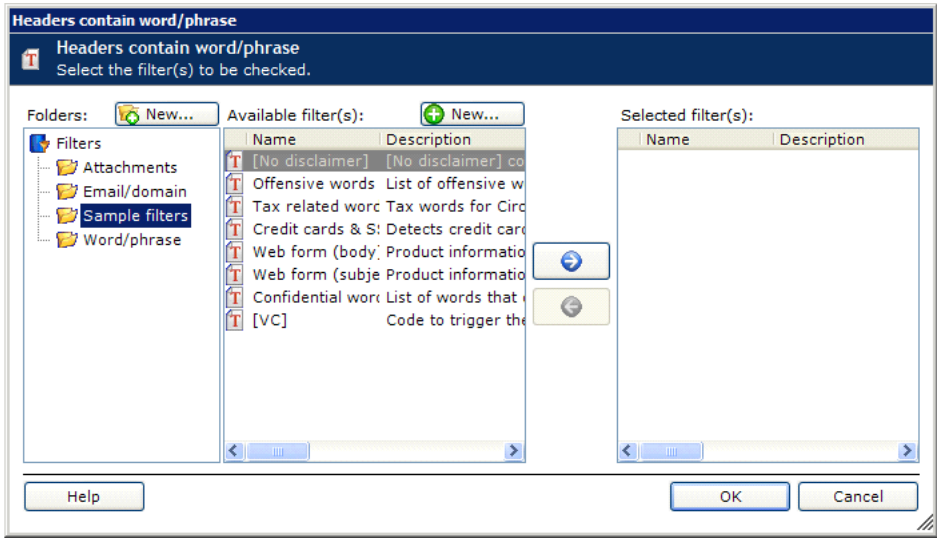


☑ **Message contains number of recipients**: Specify whether the total recipient count (the number of recipients in the To: and Cc: fields) should be equal to or greater than, less than, between or not between a certain value. If you select **is greater than** or **is less than**, the value itself will not be included. For instance, if you specify that a policy should trigger when there are more than 2 recipients, the policy will trigger for messages with 3 or more recipients. If you select **is between** or **is not between**, this will include the two values. For instance, if you select **is between** 2 and 4 recipients, the policy will trigger for messages with 2, 3 and 4 recipients. If you select **is not between** 2 and 4

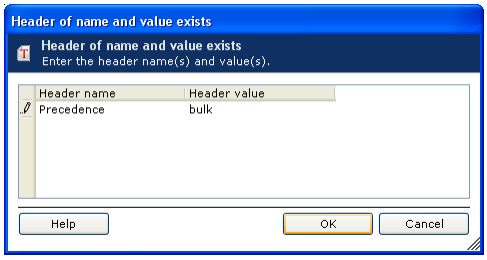
recipients, the policy will not trigger for messages with 2, 3 and 4 recipients. Policy Patrol cannot count bcc: recipients. Distribution lists will be counted as one recipient.



☑ **Headers contain word/phrase**: Select the filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol will search all headers for the word(s) in the filter.



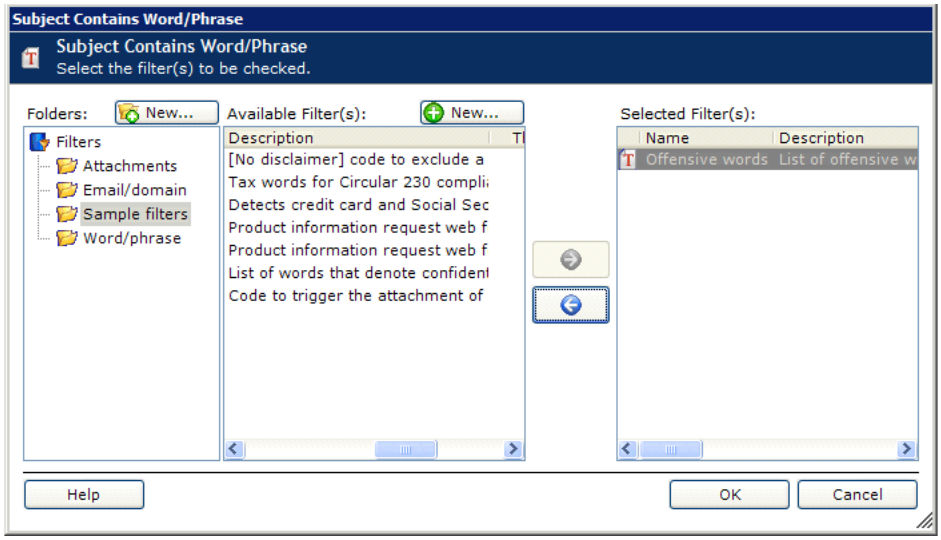
☑ **Header of name and value exists**: Enter the header name and value that Policy Patrol must search for.



- **Subject**

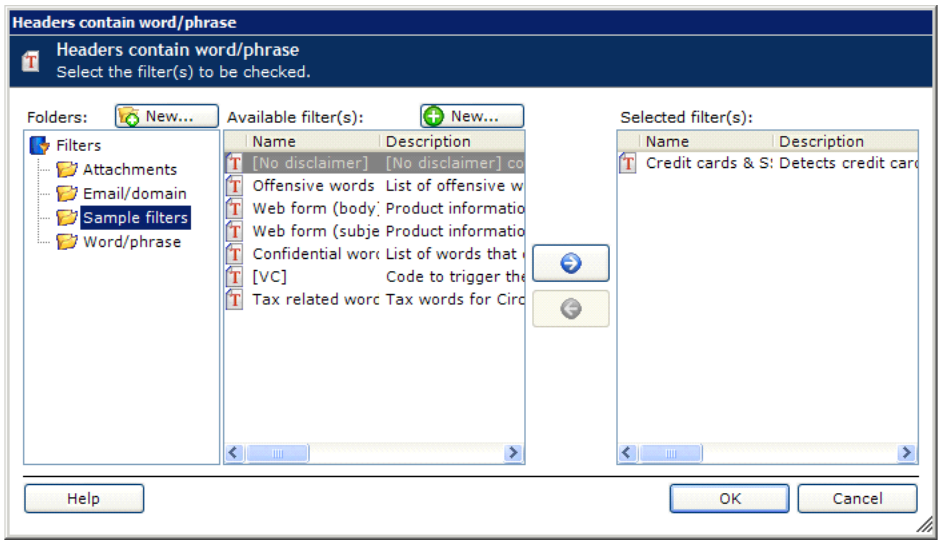
☑ **Subject is missing or empty**: Check this option if you wish the policy to trigger when a message has an empty subject or no subject field at all.

☑ **Subject contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list.



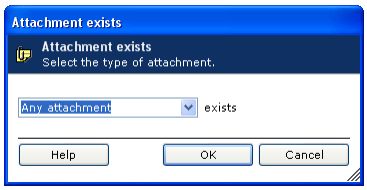
- **Body**

☑ **Body contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folders list. If you wish to check the HTML source code, check the option **Check HTML tags**. This can be useful if you want to check for scripts by searching for the `<SCRIPT>` tag. If you wish to check normal text, do not select this option since it will produce unwanted results.



- **Attachment**

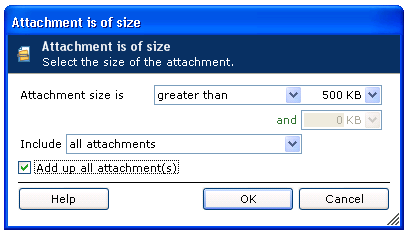
☑ **Attachment exists**: Select whether you wish to check for **any attachment**, **inline attachment** (embedded pictures) or **standard attachment** (files that have been attached to the message).



Note

Inline attachments are pictures or objects that have been inserted in the email message itself. Non-inline attachments are files that have been attached to the message.

☑ **Attachment is of size**: Specify whether the attachment should be **greater than**, **less than**, **between** or **not between** certain values. By default each attachment to the message is counted separately. So if you have a policy that triggers when an attachment is greater than 1 MB, the policy will not trigger for a message that includes two attachments of 550 KB each. If you wish to check the total size of attachments to the message, you must select the option **Add up all attachments**. Specify whether you wish to check for **all attachments**, **inline attachments only** (embedded pictures) or **standard attachments only** (files that have been attached to the message).



☑ **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 CLSID extension.

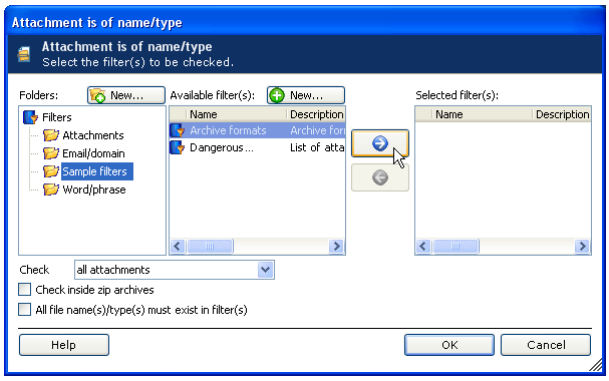
Attempt to verify attachment extension: Policy Patrol can verify over 100 file types. A list of files that Policy Patrol can verify is found in **Settings** > **Attachment Maps**. For instance, if a user tries to circumvent a policy blocking exe files and renames the `virus.exe` file to `virus.doc`,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

Check for binary text files: 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.

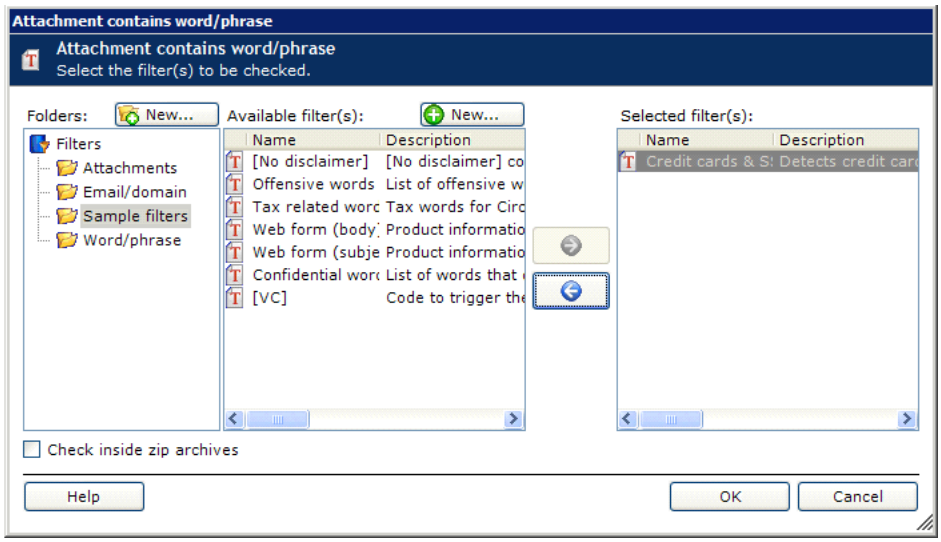
☑ **Attachment is of name/type**: Select the attachment filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Specify whether you wish to check for **all attachments**, **inline attachments only** (embedded pictures) or **standard attachments only** (files that have been attached to the message). If you want Policy

Patrol to check attachments within zip files, check the option **Check inside zip archives**. If you wish all file names/types to exist in the filter in order to trigger the condition, check the option **All file name(s)/type(s) must exist in filter(s)**.

> **Note**
>
> If you create a policy that allows only safe attachments to be received, you must check the option **All file name(s)/type(s) must exist in filter(s)**. If you did not check the option, messages with at least one safe attachment would be let through no matter whether the other attachments were safe. Note: do not check the option **All file name(s)/type(s) must exist in filter(s)** when you are blocking dangerous attachments. Checking this option would mean that the message would not be blocked if it contained safe attachments as well as dangerous attachments.



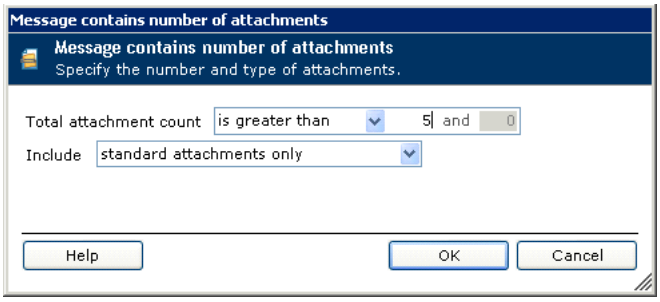
☑ **Attachment contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol can check text and html documents. If you want Policy Patrol to check attachments within zip files, check the option **Check inside zip archives**.



Note that by default Policy Patrol can only content check .txt files and .html files. If you wish Policy Patrol to content check other attachment types such as Microsoft Word or PDF files, you must install the appropriate IFilters on the Policy Patrol machine. IFilters can be downloaded from the following web pages:

- Microsoft Office: http://www.microsoft.com/downloads/details.aspx?FamilyId=60C92A37-719C-4077-B5C6-CAC34F4227CC&displaylang=en.
- Pdf: http://www.adobe.com/support/downloads/detail.jsp?ftpID=2611 (32-bit) and http://www.adobe.com/support/downloads/detail.jsp?ftpID=4025 (64-bit)
- Other IFilters: http://www.ifilter.org/Links.htm

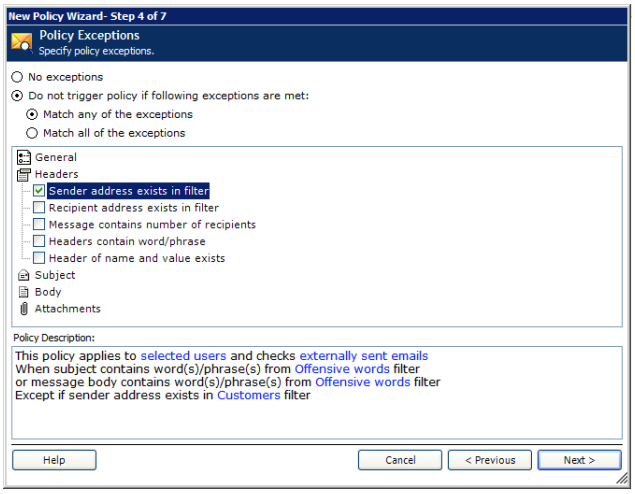
☑ **Message contains number of attachments**: Specify whether the number of attachments must **equal** or be greater than, less than, between or not between a certain value. If you select **is greater than** or **is less than**, the value itself will not be included. For instance, if you specify that a policy should trigger when there are more than 2 attachments, the policy will trigger for messages with 3 or more attachments. If you select **is between** or is **not between**, this will include the two values. For instance, if you select **is between** 2 and 4, the policy will trigger for messages with 2, 3 and 4 attachments. If you select **is not between** 2 and 4, the policy will not trigger for messages with 2, 3 and 4 attachments. Specify whether you wish to check for **all attachments**, **inline attachments only** or **standard attachments only**.



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

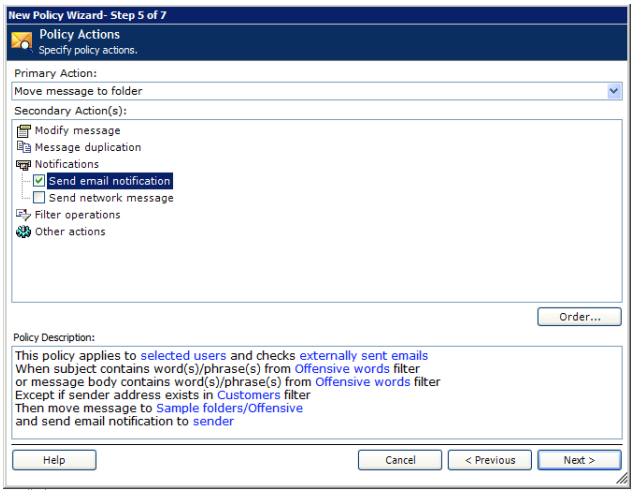
8.1.4 Step 4. Policy Exceptions

If the policy has no exceptions, leave the option **No exceptions** enabled. To specify exceptions, select **Do not trigger policy if following exceptions are met**. The options will now be the same as in step 3. When you are ready specifying exceptions, click **Next**.



8.1.5 Step 5. Policy Actions

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. Secondary actions are additional actions and are not mutually exclusive. Therefore you can configure as many secondary actions as you wish.

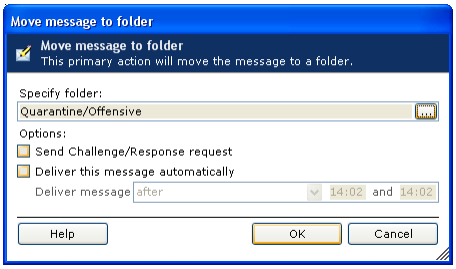


8.1.5.1 Primary Actions

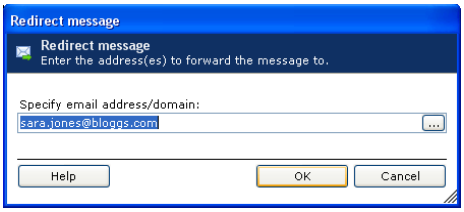
Three primary actions are available:

1. **Deliver message**: This option will deliver the message (with any secondary actions applied).

2. **Move message to folder**: This option will move the message to a monitoring folder for further review. Click on the **folder** link and select the folder where the message should be moved to. If you want to send a challenge/response request (this is used for spam management and sends an email to the sender asking them to click on a web link and verify the message), select the option **Send Challenge/Response request**. If you want to deliver the message within a specific time, select the option **Deliver this message automatically**, select **after** or **between** and enter the time(s). You can also select to deliver/delete/move the message from the folder after a specified time frame, e.g. five minutes or one day. This can be configured from the monitoring folder properties, as described in the chapter 'Quarantined messages'.



3. **Redirect message**: Select this option to forward the message to an alternative recipient. Enter the new recipient email address. Multiple recipients must be separated by a semi colon, i.e. ;.

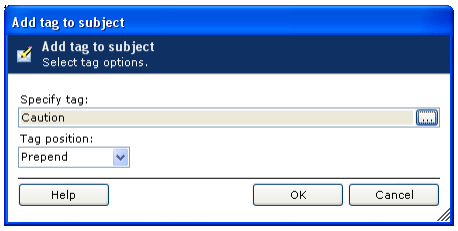


8.1.5.2 Secondary Actions

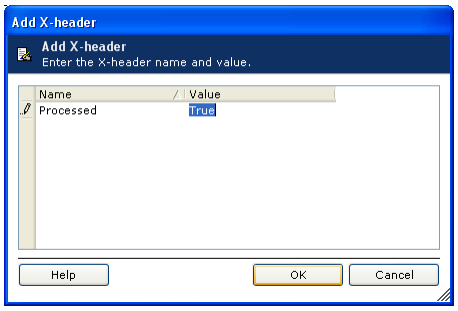
The following secondary actions are available:

- **Modify message**

  ☑ **Add tag to subject**: This option allows you to add a tag to the subject. Click on the **...** button to select a tag. For instance, as a warning to users you could add the tag 'CAUTION: POSSIBLE VIRUS'. You can choose 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]. If you want to have a space between the tag and the subject, you must enter this in the tag template.



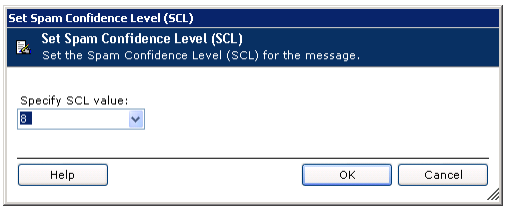
☑ **Add X-header**: This option can be used to add an X-header of a certain value to the mail. This can be of use if you wish an application to automatically process the mail or if you want to further process the message with an Outlook rule. In the options, enter the X-header to be added and the corresponding 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.



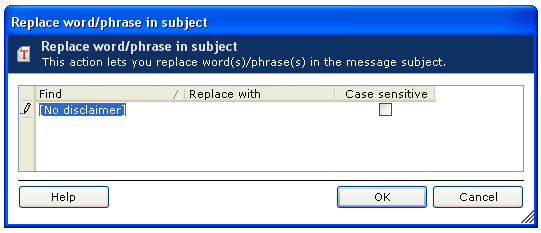
Tip

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.

☑ **Set Spam Confidence Level (SCL)**: This option will assign an SCL value to the message that Outlook 2003/2007/2010/2011/2013 can use to determine what action to take for the message. The SCL value can be from 0-9, with 0 indicating a legitimate message and 9 indicating a spam message. The value -1 indicates that the message is white listed. It is also possible to increase the SCL value with a value from 1 to 9. To do this, select one of the options **Increase by n**, where n is the number to increase the value by. This can be useful if you are for instance using spam filtering on Exchange Server that adds an SCL value and you want to use Policy Patrol as an additional anti spam layer. If Policy Patrol considers the message spam, it can for instance increase the SCL value with 3. If the message already had an SCL value of 4, the new SCL value will be 7. Note that this feature requires Exchange 2003 or higher.



☑ **Replace word/phrase in subject**: Select this option to replace a word or phrase in the subject. Enter the words or phrases to be replaced in the 'Find' 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 policy 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 [No disclaimer]. You can then create a policy in Policy Patrol that a disclaimer is added unless the subject contains the word [No disclaimer]. A further policy can be created to remove the code [No disclaimer] from the subject so that the recipient does not see the code in the subject.

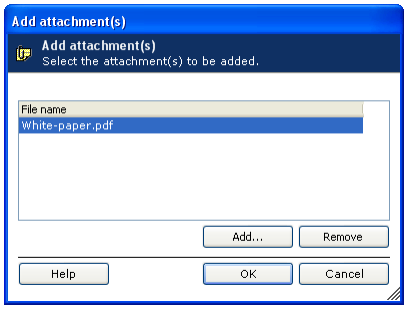
☑ **Convert message body to plain text**: This option will convert the message to plain text. You might wish to do this to save bandwidth, or to remove any possible HTML embedded viruses. There are no further options for this action. Note: Policy Patrol for Exchange 2007/2010/2013 64-bit can only convert external messages to plain text, not internal messages.

☑ **Attach 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.

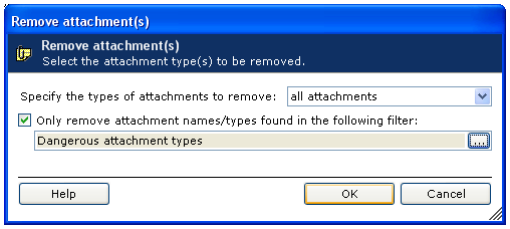
☑ **Remove read receipt request**: If you select this option, Policy Patrol will remove the read receipt request.

☑ **Remove delivery receipt request**: If you select this option, Policy Patrol will remove the delivery receipt request.

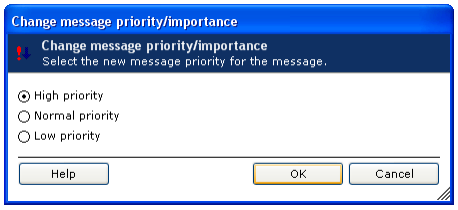
- **Add attachment(s)**: This option adds an attachment to the original message. Click **Add** to select the attachment(s) to be added. Enter the path to the file or click on … to browse to the file (Remember that the file must reside on the same machine as Policy Patrol). Click **OK**. Repeat the process if you want to add multiple attachments to the message. When you are done, click **OK** to close the dialog.



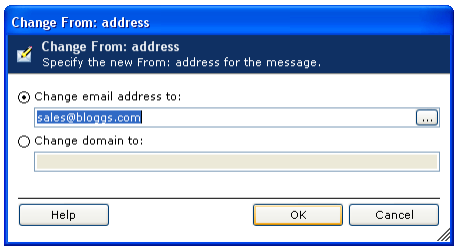
- **Remove attachment(s)**: Select this option to remove attachments from the message. Select which attachments you wish to remove: **all attachments**, **inline attachments only** (embedded pictures) or **standard attachments only** (files that have been attached to the message). If you do not want to remove all attachments but only a certain type of attachments, select the option **Only remove attachment names/types found in the following filter**. Click on the **...** button and select the attachment filter.



- **Change message priority/importance**: With this option you can change the priority or importance of the message. Select **High priority**, **Normal priority** or **Low priority**.

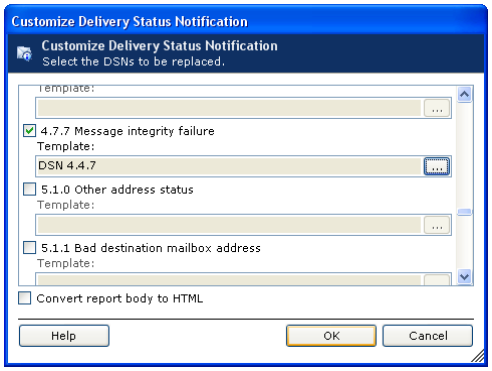


- **Change From: address**: Select this option if you wish to change the From: domain or email address. You might want to change this if you want to use a generic reply address such as sales@domain.com, instead of the specific user's email address. To change the From: email address, select **Change email address to:** and enter the new email address. If you also want a display name to be shown, enter it as follows: `"Display name" <user@domain.com>`. To change the From: domain, select **Change domain to:** and enter the new domain (the original display name will be shown). Note that this option only works for externally sent messages.



- ☑ **Change Reply to: address**: Select this option if you wish to change the Reply to: address of the message. For instance, you might want to use an individual email address in the From: field, but use a generic email address such as sales@company.com in the Reply-to: address so that the email gets logged in the CRM system. Note that this option only works for externally sent messages. To change the Reply to: email address, select **Change email address to:** and enter the new email address. If you also want a display name to be shown, enter it as follows: `"Display name" <user@domain.com>`. To change the Reply to: domain, select **Change domain to:** and enter the new domain (the original display name will be shown). Note that this option only works for externally sent messages.

- ☑ **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 **Other** 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 **Convert report body to HTML**. Policy Patrol will then use the text you entered in the HTML tab of the Template. Note that even though most clients can read HTML, there are still some clients, such as UNIX clients that may not be able to read HTML mail. If you wish Delivery Status Notifications to be sent in plain text only, leave the **Convert report body to HTML** checkbox unchecked (not applicable to the 64-bit version).

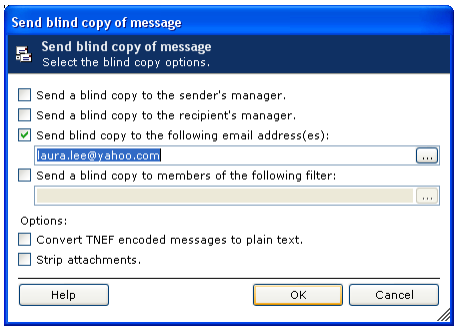


Note

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

- **Message duplication**

☑ **Send blind copy of message**: 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. To send a blind copy to an email address, select **Send blind copy to the following email address(es)** 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. If you wish to enter multiple addresses they must be separated by a semi colon. You can also send a copy to the sender's or recipient's manager, or send a copy to recipients in a filter.



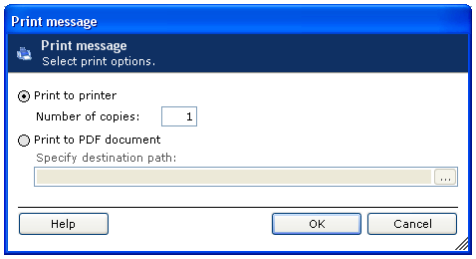
Note

If you want to send a copy of an internal message to an external recipient, you must tick the option **Convert TNEF encoded messages 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.

If you do not want to include attachments in the blind copy, check the option **Strip attachments**.

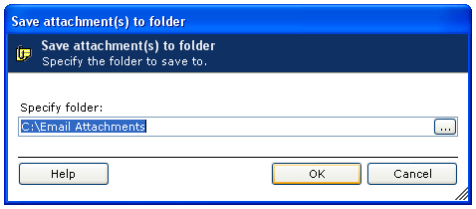
☑ **Print message**: Select this option to print the message or convert it to a PDF file. To print your message, select **Print to printer** and enter the number of copies that should be printed. Policy Patrol will print the message to the default printer.

If you wish to convert the message to pdf, select **Print to PDF document** and enter the destination path.

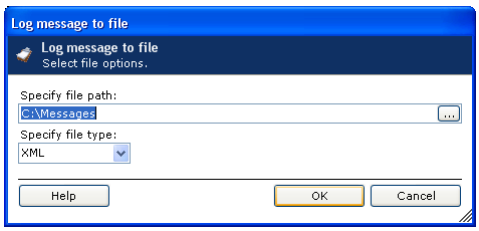


☑ **Save attachment(s) to folder:** By selecting this option Policy Patrol will save the attachment(s) to the specified folder. If an attachment name already exists, Policy Patrol will add the suffix 'nnn'. For instance, if an attachment Document.doc is sent for the

second time, the second file name will be called Document001.doc, the third will be called Document002.doc, etc.

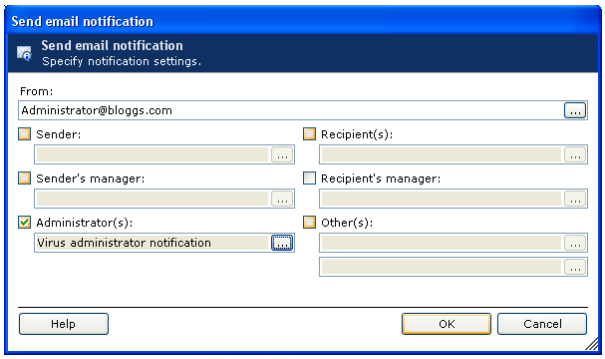


☑ **Log message to file:** Select this option if you wish to log messages to a file. Enter the file path where the log files will be stored and select to save in CSV or XML format. A new file will be created daily with the following name: PP4_MSGyyyymmdd.xml, i.e. PP4_MSG20051025.xml or PP4_MSGyyyymmdd.csv, i.e. PP4_MSG20051025.xml.



- **Notifications**

☑ **Send email notification**: By selecting this option, Policy Patrol will send a notification message. Click on the link in the description and enter or select a From: address. If you wish a display name to appear in the notification message, enter "Display name" <email address>, e.g. `"John Doe" <John.Doe@company.com>`. Now specify who should receive the notification (sender, recipient(s), administrator, sender's manager, recipient(s)' manager or other(s)) and select the template to be used for each recipient. If you wish to use a new template, click **New...**.

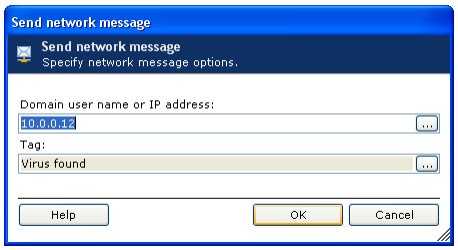


Note

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>** > **Advanced** > **System configuration** > **System notifications**.

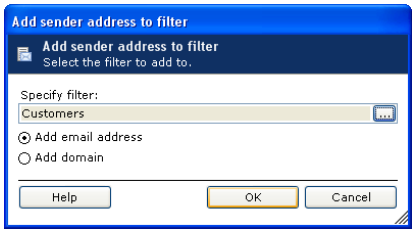
☑ **Send network message**: Select this option to send a network message. Click on the link in the description and enter the user name or IP address of the computer you wish to send a network message to. In **Tag**, select the message to be sent by clicking on **...**. Note that this option is not available in Policy Patrol for Exchange 2007/2010/2013 (64-bit version).



- **Filter Operations**

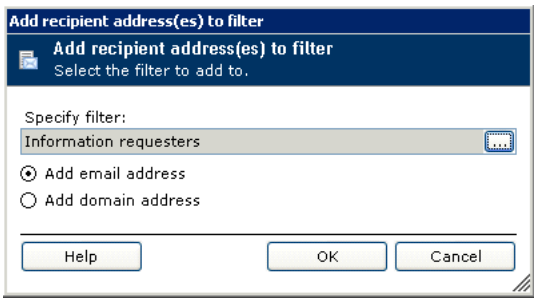
☑ **Add sender address to filter**: This option will add the From: domain or email address to a predefined filter. This can for instance be useful to avoid multiple auto reply emails. For more information on configuring auto replies please consult the following document:

Email management with Policy Patrol
(http://www.policypatrol.com/assets/pp10-emailmanagement.pdf)

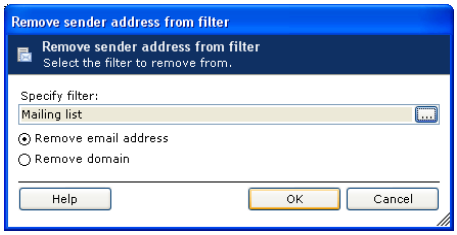


Click on **...** to select the filter to add the From: domain or email address to. If you wish to create a new filter, click the **New** button above the filter list. If you wish to create a new folder, click the **New** button above the folder list. To view the properties of a configured filter, right-click the filter and select **Edit**. Select **Add email address** if you wish to add the email address to the filter and select **Add domain** to add the domain to the filter. The addresses in the From: and X-Sender fields will be added.

☑ **Add recipient address(es) to filter**: This option will add the recipient domain or email address to a predefined filter. Click on **...** to select the filter to add the recipient domain/email address to. If you wish to create a new filter, click the **New** button above the filter list. If you wish to create a new folder, click the **New** button above the folder list. To view the properties of a configured filter, right-click the filter and select **Edit**. Select **Add email address** if you wish to add the email address to the filter and select **Add domain** to add the domain to the filter. The recipient addresses specified in the To:, Cc: and X-Receiver fields will be added.



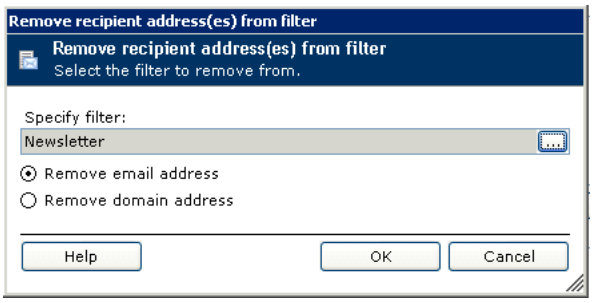
☑ **Remove sender address from filter**: This option removes the sender domain or email address from a selected filter and can be used for managing mailing lists. Click on **...** and select the filter. If you wish to create a new filter, click the **New** button above the filter list. If you wish to create a new folder, click the **New** button above the folder list. To edit a configured filter, right-click the filter and select **Edit**. Select **Remove email address** if you wish to remove the email address from the filter and select **Remove domain** to remove the domain from the filter. The sender addresses in the From: and X-Sender fields will be removed.



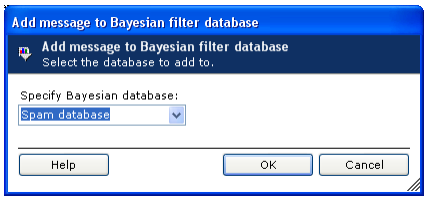
Tip

This action can be used to maintain lists of subscribers to newsletters. To unsubscribe, subscribers can send an email to a particular address with unsubscribe in the subject. When this email message is received, Policy Patrol can remove the sender from the newsletters list.

☑ **Remove recipient address(es) from filter**: This option removes the recipient domain or email address(es) from a selected filter. If you wish to create a new filter, click the **New** button above the filter list. If you wish to create a new folder, click the **New** button above the folder list. Click on the link, select the filter and specify whether to remove the domain or email address. The recipient addresses specified in the To:, Cc: and X-Receiver fields will be removed.



☑ **Add message to Bayesian filter database**: Select this option if you wish to add the message to the Bayesian filter database. Although all outgoing messages are automatically added to the legitimate Bayesian filter database when **Enable automatic Bayesian filter learning** is enabled, this option can be used to place incoming mail for honey pots into the spam database.

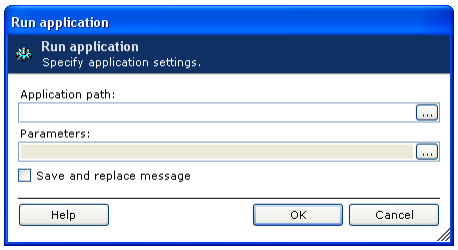


Tip

If you have mailboxes for ex-employees, these frequently continue to receive spam but no longer receive legitimate mail. Messages for these users can be placed in the Bayesian filter spam database unless they are still receiving legitimate messages, for instance newsletters.

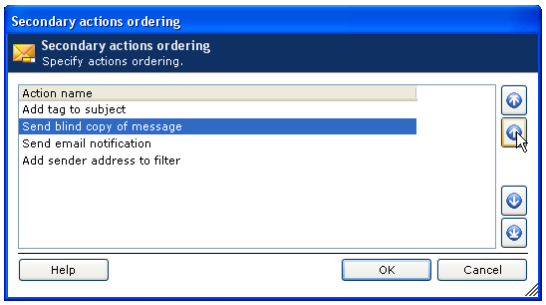
- **Other Actions**

☑ **Run application**: You can use this option to run an external program, for instance to send an SMS message or to beep a pager. You can also use this action to scan the message with an anti-virus command line scanner. Enter the path and file name or browse to the application to be executed by Policy Patrol. Enter the application name and optionally any parameters to be used. Click on the **...** to create a tag with the parameters. The parameters can include fields such as the subject or sender of the message or the name of the virus found. By default Policy Patrol always adds the path and file name of the message currently being processed as the first parameter. If you wish to replace the original message with the changes that were made, select **Save and replace message**. This means that the modified message will be delivered.



8.1.5.3 Ordering of Secondary Actions

By default Policy Patrol will apply the secondary actions in random order. However, sometimes it can be important that the actions are applied in a certain order. For instance if you want your printed message to include a subject tag, the 'Add tag to subject' action must be ordered above the 'Print message' action. To change the order of the secondary actions, click on **Order...**. Then select the action and press the **Move up** or **Move down** buttons.

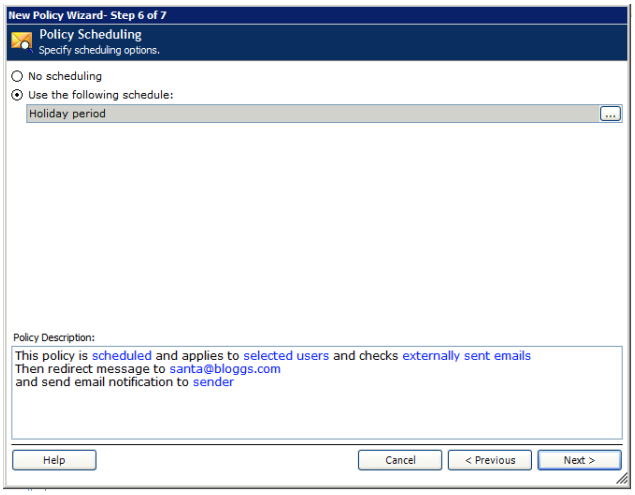


Note

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.

8.1.6 Step 6. Policy Scheduling

A policy can be scheduled to run on certain days, times, and dates. If you do not wish to schedule the policy, select **No scheduling** and click **Next**. If you wish to schedule the policy, select **Use the following schedule** and select the schedule from the drop down list. If you wish to create a new schedule, click **New**. For more information on how to create schedules, please consult paragraph 18.3. 'Schedules'.

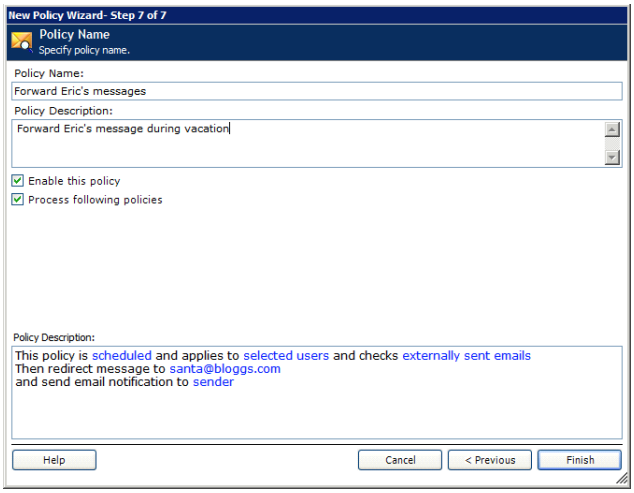


Tip

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

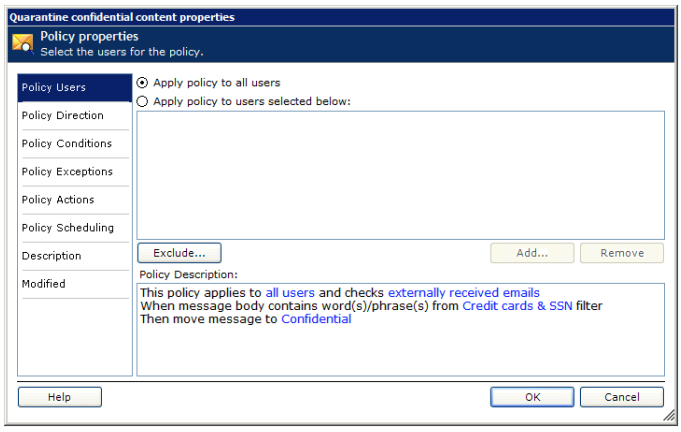
8.1.7 Step 7. Policy Name

In the final step, enter a name for the policy and any comments. Uncheck **Enable this policy** if you do not want the policy to be enabled right away. If you do not want any following policies to be processed once this policy has triggered, uncheck the option **Process following policy(s)**. Click **Finish** to create the policy.



8.2 Editing Existing Policies

To edit an existing rule, go to **Email Content Policies** and select the policy to be edited. Double-click on the policy or click on the **Edit** button. A dialog with several tabs will appear. Make the changes in the appropriate tabs.



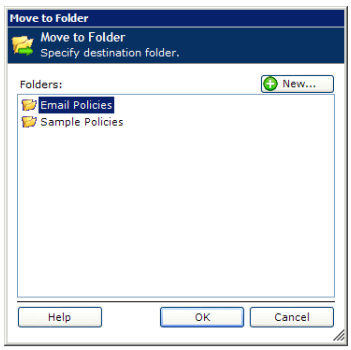
If you want to change the name of a policy, right-click the policy in the list and select **Rename**. If you want to move a policy to another folder, right-click the policy and select **Move**. Select the folder you wish to move the policy to and click **OK**.

8.3 Copying Policies

To copy an existing policy, right-click the policy and select **Duplicate**. The policy will now be duplicated. The name will be displayed as follows: Copy of <original policy name>.

8.4 Moving Policies

To move a rule to a different folder, right click on the policy and select **Move**. Select the folder you wish to move the policy to and click **OK**. To create a new folder, click the **New...** button.



Chapter 9

Email Signatures

Policy Patrol allows you to add email disclaimers, personalized email signatures and HTML Stationery to your emails. This chapter describes how to configure the disclaimer, email signature and HTML stationery policies.

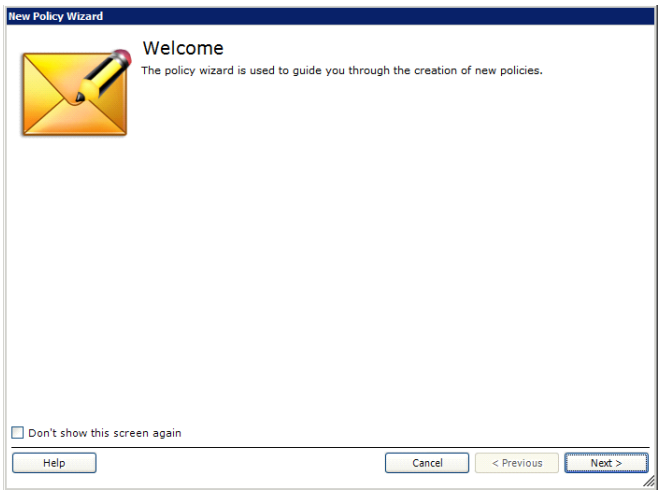
9.1 Configuring a Signature Policy

To configure a new policy, go to **Email Signatures**, select the appropriate folder and click **New...**. If you wish to create a new folder, right-click on **Email Signatures** and select **New folder...** In the folder click on the **New...** button.

Note

Remember that you must first select a folder before you can create a new policy.

The policy wizard will appear. In the Welcome screen, click **Next.**



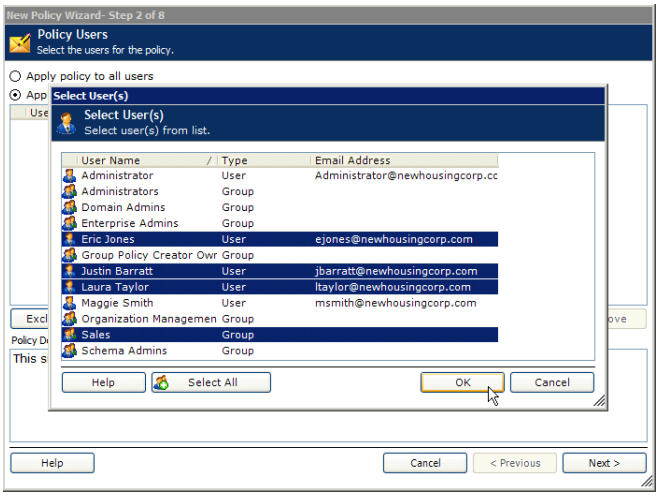
The policy wizard will now guide you through the different steps described below.

? Info

From step 2 onwards. the wizard is divided into two panes. The policy options are displayed in the top pane and the policy description in the bottom 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 for a selected option, a dialog will pop up asking you to specify further options. Once a value is set, the link color will appear in blue in the bottom pane. If you do not select a value, the link will appear in red since it still needs to be configured. If you have not yet set all values when you click finish to create your policy, a warning will pop up. You will still be able to create the policy, but the policy will not be enabled until you set all values.

9.1.1 Step 1. Policy Users

To apply the policy globally, select **Apply policy to all users**. To apply the policy to certain users, groups, or domains select **Apply policy to users listed below** and click **Add...** Select the users for the policy. To select multiple users, hold down the [CTRL] or [SHIFT] keys or use the **Select all** button. When you have selected the users for the policy, click **OK**. To remove users from the policy, select the user(s) and click **Remove**. If you wish to add exceptions, for instance if you wish the policy to apply to all users apart from the Board of Directors, click on **Exclude...** and **Add...**. Select the user(s) to exclude, click **OK** and **Close**. Click **Next**.

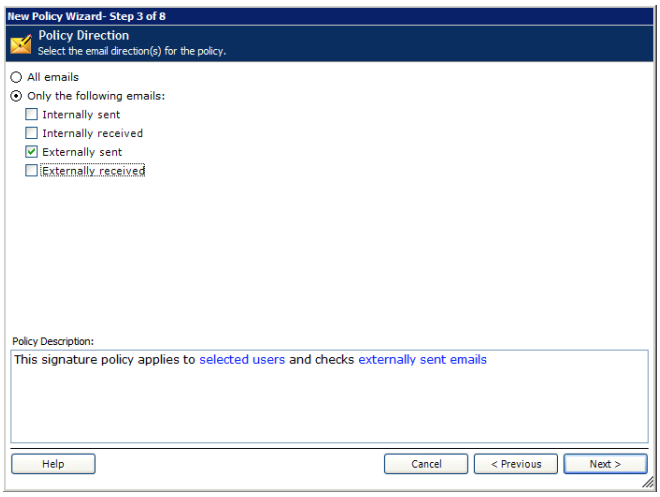


Tip

If you wish to configure a policy for a domain or for users that have a certain Active Directory attribute, you can create a manual input group and select this from the list. For more information on how to create this group, consult the instructions in paragraph 4.41 (for a domain) and 4.4.2 (for an LDAP query).

9.1.2 Step 2. Policy Direction

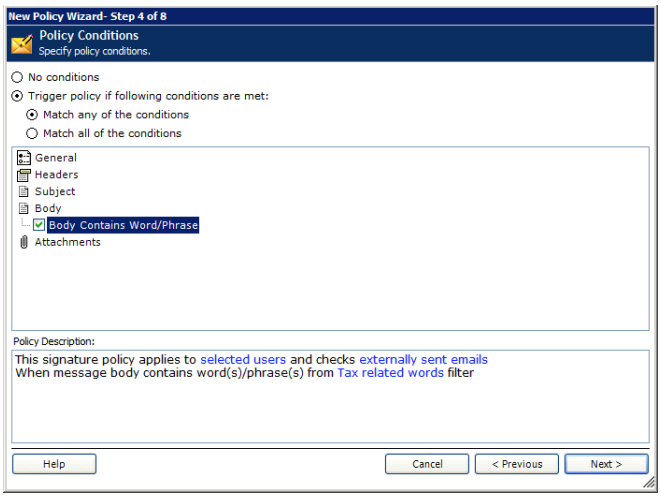
Specify whether you wish to apply the policy to all messages or only internally sent and/or received messages, and/or externally sent and/or received messages. Remember that Policy Patrol can only apply policies to internal messages if you have installed Policy Patrol on an Exchange Server machine. Click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



9.1.3 Step 3. Policy Conditions

Here you must specify which conditions should be met for the policy to trigger. If the policy should always trigger (for instance if you want to add a signature to all messages), leave **No conditions** selected and click **Next**. If the policy should only trigger in certain circumstances, select **Trigger policy if following conditions are met**. The different conditions are sorted into the following classifications: 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 add a disclaimer when certain words are found in the body or subject, 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 a disclaimer when certain words are found in the body as well as the subject.



Available conditions:

- **General**

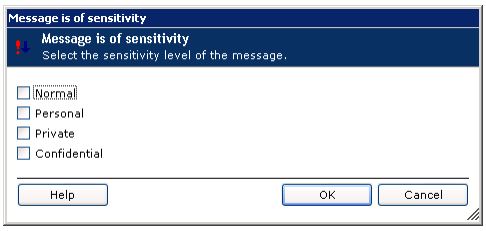
  ☑ **Message is encrypted**: This condition checks whether a message is encrypted.

  ☑ **Message is digitally signed**: This condition checks whether a message is digitally signed.

  ☑ **Message is of priority/importance**: Specify whether the message should be of High, Normal and/or Low priority.



  ☑ **Message is of sensitivity**: Specify whether the message should be Normal, Personal, Private and/or Confidential.

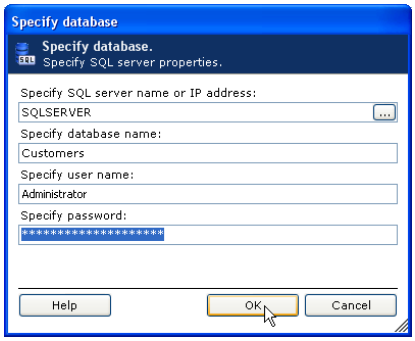


  ☑ **Message is DSN report**: Specify whether the message should be a Success, Delay, Failure notification, or Other report (report without status code).

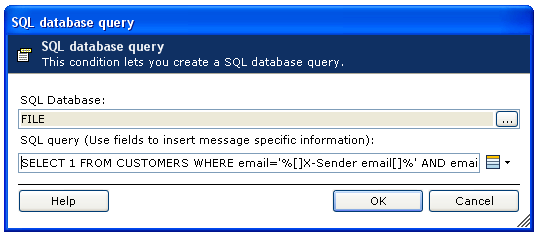
Note

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 Policy Wizard.

☑ **Message matches SQL database query:** This condition allows you to look up information in a SQL database and search for this information in any message or user field. For instance you could use this condition to trigger a policy only when senders or recipients are found in the database. Firstly you need to specify the SQL database settings by clicking on …



Enter the SQL Server name or IP address, or click on **…** to browse to the machine. Enter the database name and enter the user name and password for accessing the database. Click **OK**.



Now you must enter the SQL query in the following format:

SELECT 1 FROM [SQL_table_name] WHERE [column_name]=%[]Message field[]%

Where:

[SQL_table_name] = name of the table in SQL Server to look up information from

[column_name] = name of the table column where you want to look up information

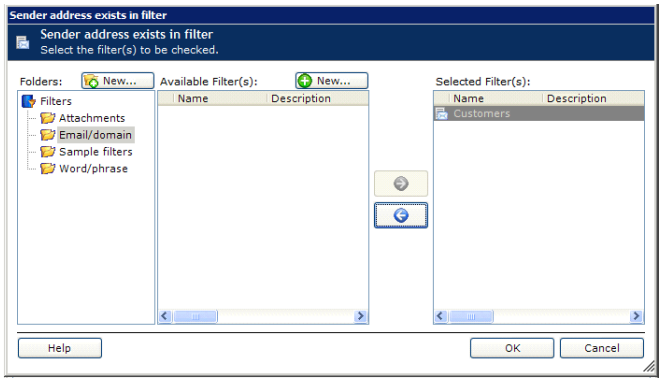
%[]Message field[]% = Message field that you want to match in the SQL table column

For instance, you have a SQL table called CUSTOMERS and in the 'Email' column you have listed all your customers' email addresses. To trigger a policy that applies only to emails sent to email addresses in the CUSTOMERS table, excluding those entries in the database without an email address, you must enter the following query:

```
SELECT 1 FROM CUSTOMERS WHERE Email='%[]X-Receiver email[]%' AND email <> ''
```

- **Headers**

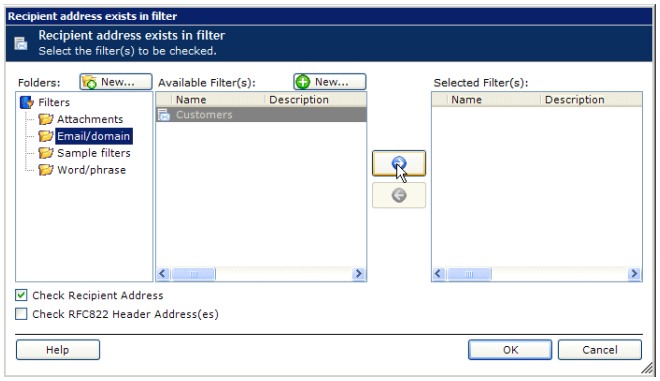
☑ **Sender address exists in filter**: Select the Email/domain filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol will check the From: and X-Sender fields for the configured address(es).



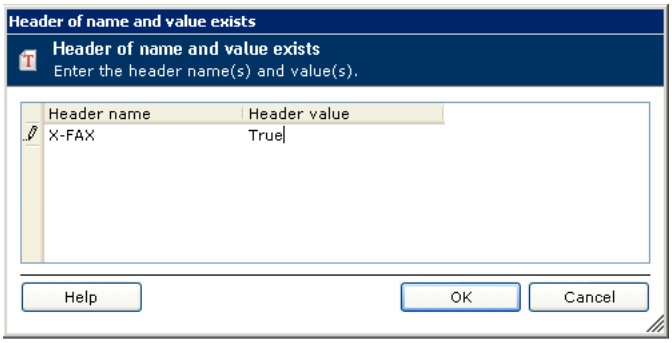
Note

The predefined filters folder contains the Email block list and Email allow list filter. These lists are configured from Anti-spam > Block/Allow. If you wish to handle spam messages via the policies you can select these filters if you wish.

☑ **Recipient address exists in filter**: Select the Email/domain filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. If you wish Policy Patrol to check the X-Receiver field, select the option **Check recipient address**. If you wish to check the To: and Cc: fields, enable the option **Check RFC822 header address(es**).

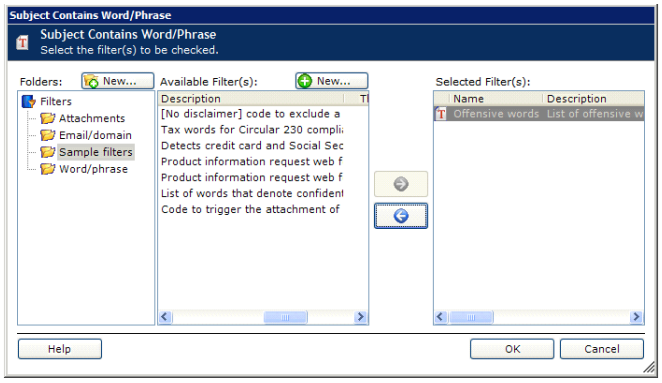


☑ **Header of name and value exists**: Enter the header name and value that Policy Patrol must search for.



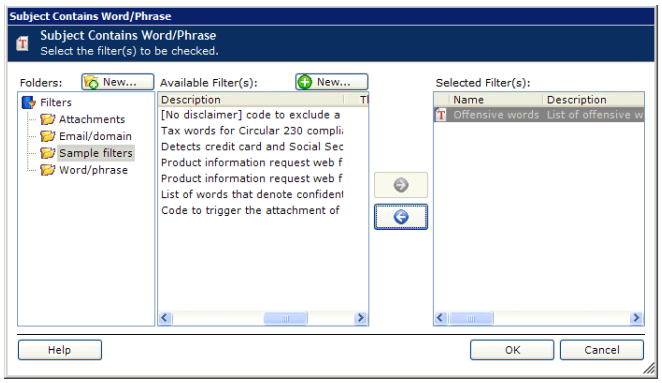
- **Subject**

☑ **Subject contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list.



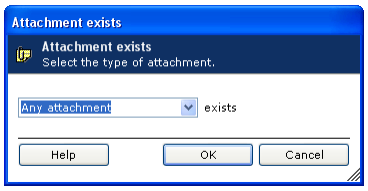
- **Body**

☑ **Body contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folders list. If you wish to check the HTML source code, check the option **Check HTML tags**. This can be useful if you want to check for scripts by searching for the `<SCRIPT>` tag. If you wish to check normal text, do not select this option since it will produce unwanted results.



- **Attachment**

  ☑ **Attachment exists**: Select whether you wish to check for **any attachment**, **inline attachment** (embedded pictures) or **standard attachment** (files that have been attached to the message).



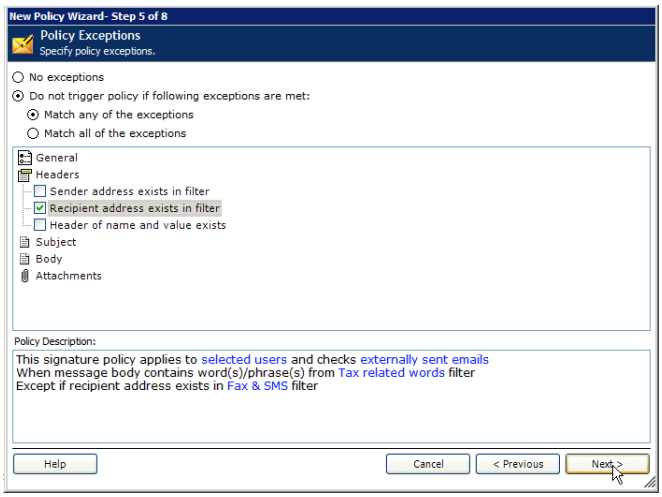
Note

Inline attachments are pictures or objects that have been inserted in the email message itself. Non-inline attachments are files that have been attached to the message.

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

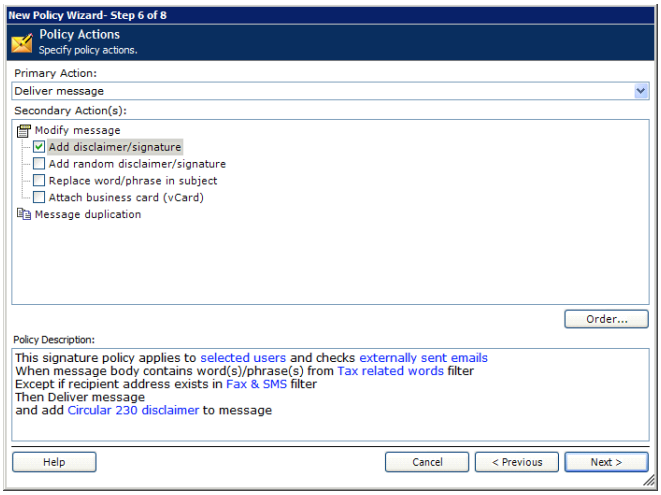
9.1.4 Step 4. Policy Exceptions

If the policy has no exceptions, leave the option **No exceptions** enabled. To specify exceptions, activate **Do not trigger policy if following exceptions are met**. The options will now be the same as in step 3. Policy exceptions can for instance be used to exclude faxes and SMS messages from the signature policy. When you are ready specifying exceptions, click **Next**.



9.1.5 Step 5. Policy Actions

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. Secondary actions are additional actions and are not mutually exclusive. Therefore you can configure as many secondary actions as you wish.



9.1.5.1 Primary Actions

For a signature policy, the primary action is set to **Deliver message**. This option will deliver the message after the secondary actions are taken.

9.1.5.2 Secondary Actions

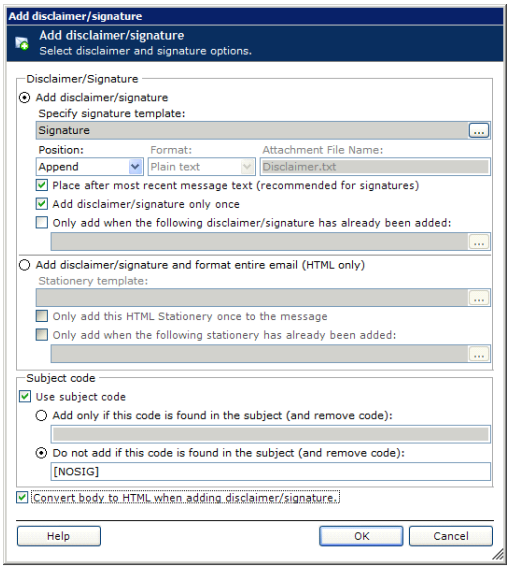
The following secondary actions are available:

- **Modify message**

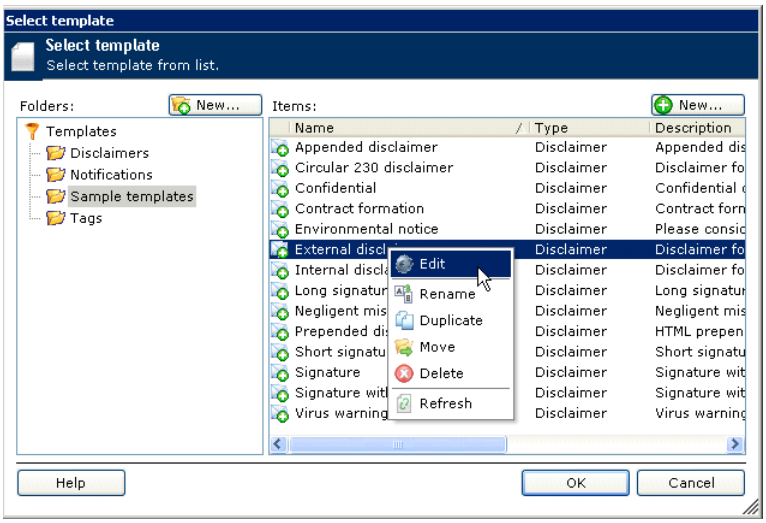
☑ **Add disclaimer/signature**: This option will add a disclaimer or signature to the message. There are two ways in which Policy Patrol can add an email disclaimer or email signature. The option **Add disclaimer/signature** allows you to add a block of text at the bottom or top of an email (or below the most recent message text), but it does not change the actual email body text. The option **Add disclaimer/signature and format the entire email (HTML only)** allows you to format the entire email and add headers, footers and sidebars. The actual email text will be inserted into the HTML Stationery template. Both options are explained below.

❑ Add disclaimer/signature

This option allows you to add a block of text at the bottom or top of an email (or below the most recent message text).



Under 'Specify signature template', click on the **...** button to select the Signature template that you wish to add. If you want to preview or edit the disclaimer template, right-click and select **Edit**. If you wish to create a new signature template, click on the **New** button above the template list. To create a new folder, click on the **New** button above the folder list. When you are done, click **OK**.



Specify the disclaimer/signature position by selecting **Prepend**, **Append** or **Attach**. If you select to attach the disclaimer you must specify the file format and name. Remember that if you select Plain text format, the signature template must include text in the RTF/Plain tab. If you select HTML format, the signature template must include text in the HTML tab.

If you wish the disclaimer or signature to be placed after the last entered message text on replies and forwards, select **Place after most recent message text (recommended for signatures)**. This means that when you are replying or forwarding a message, you signature/disclaimer will be placed below the most recent message text that you entered, instead of right at the bottom of the message.

If you wish the signature or disclaimer to be added only once to the email, tick the option **Add disclaimer/signature only once**.

If you would like to only add this disclaimer/signature if a certain signature already exists, you can check the option: **Only add when the following disclaimer/signature has already been added** and select the disclaimer/signature that must already exist in the message. This option is useful if you wish to add a more extensive signature on your initial email and then a shorter signature on each additional message (see tip below).

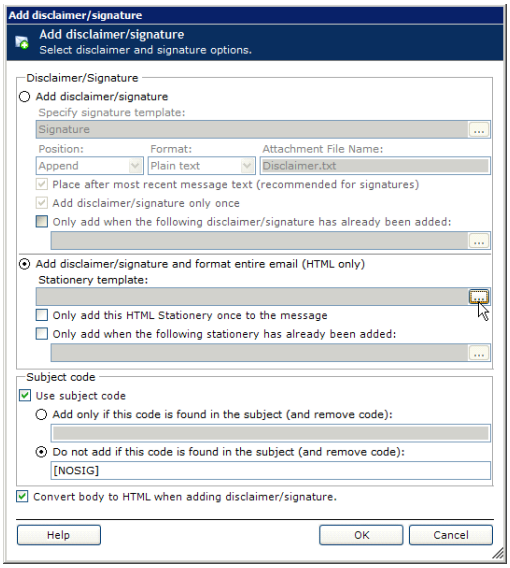
Tip

If you wish to add a more extensive signature on your first email (for instance including your complete address) and then a shorter one on each following message (for instance including only your name, company name and phone number), you can do so by first creating a policy that adds the initial, more extensive signature. In the 'Add disclaimer/signature' dialog of this policy you will select the option 'Add disclaimer/signature only once' and 'Place after most recent message text (recommended for signatures)'. Then create a second policy that adds the shorter signature. In the 'Add disclaimer/signature' options for this policy, select the options 'Place after most recent

message text (recommended for signatures)' and 'Only add when the following disclaimer/signature has already been added' and select the more extensive signature template of the first policy. In this way, any new messages will include the more extensive signature. If the initial signature has already been added to the email, any consequent messages will get the shorter signature version added.

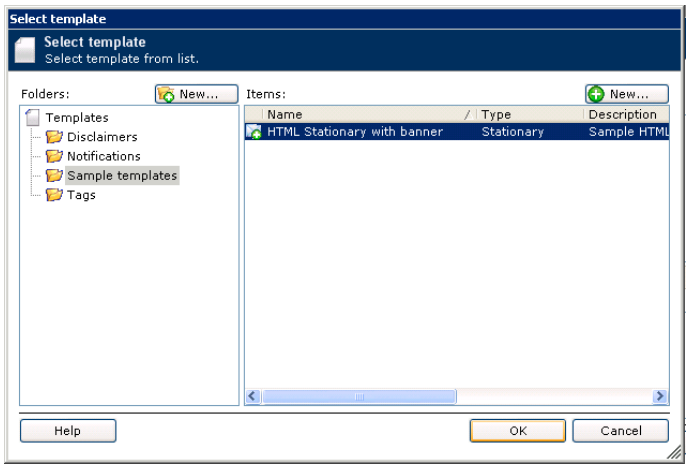
- **Add disclaimer/signature and format entire email (HTML only)**

This option allows you to format the entire email and add headers, footers and sidebars. The actual email text will be inserted into the Stationery template. Under 'Specify stationery template', click on the **...** button to select the stationery template that you wish to add. If you want to preview or edit the Stationery template, right-click and select **Edit**. If you wish to create a new template, click on the **New** button above the template list. To create a new folder, click on the **New** button above the folder list. When you are done, click **OK**.



If you only want this stationery to be added once (for instance if you wish to include the disclaimer statement only once in the email), select the option **Only add this HTML Stationery once to the message**.

If you would like to only add this HTML Stationery if a certain stationery template has already been added, you can check the option: **Only add when the following stationery has already been added** and select the stationery template that must already exist in the message. This option is useful if you wish to add the disclaimer only once to the message.



Tip

If you wish to add a different HTML Stationery Template for your first email (for instance including your disclaimer notice and complete address) and then a different one on each following message (for instance without your disclaimer statement or complete address), you can do so by first creating a policy that adds the initial stationery. In the 'Add disclaimer/signature' dialog of this policy you will select the option 'Only add this HTML Stationery once to the message'. Then create a second policy that adds the second stationery template. In the 'Add disclaimer/signature' options for this policy, select the option 'Only add when the following stationery has already been added' and select the stationery template of the first policy. In this way, any new messages will include the initial stationery. If the initial stationery has already been added to the email, any consequent messages will get the second stationery template added.

- **Subject code**

If you wish to add the disclaimer/signature/stationery only if a certain code is found in the subject, select the option **Add only if this code is found in the subject (and remove code)**. For instance, if you want users to be able to select which disclaimer/signature should be added, you can select this option and enter the agreed code for the particular signature, for instance `[SIG1]`. If `[SIG1]` is found in the subject, Policy Patrol will add the selected disclaimer/signature and will remove the code from the subject.

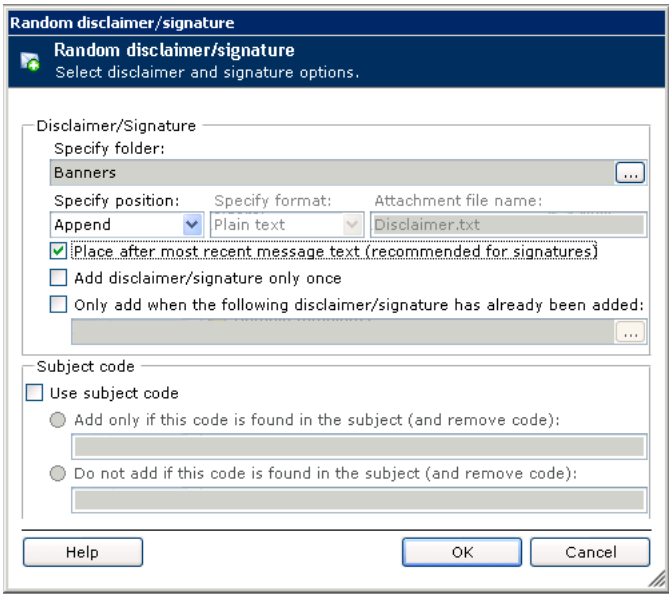
If you do not wish to add the disclaimer/signature/stationery if a certain code is found in the subject, select the option **Do not add if this code is found in the subject (and remove code)**. For instance, you can instruct users to enter the code `[No disclaimer]` in the subject if they do not want a disclaimer to be added. If this code is found, Policy Patrol will not add the disclaimer and will remove the code from the subject.

Note: You can activate both options, as long as you enter different subject codes.

- **Convert body to HTML when adding disclaimer/signature**

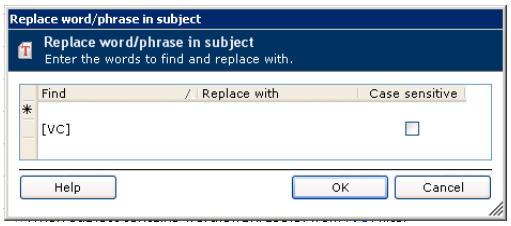
  If you wish to convert plain text emails to HTML so that the HTML signature or stationery can be added, select the option **Convert body to HTML when adding disclaimer/signature**. This is especially useful for emails sent from mobile devices: Since all mobile devices send emails out in plain text format, these emails will include a plain text signature instead of the HTML signature with formatting and pictures. By enabling this option, you will ensure that even emails sent from mobile phones will be sent in HTML format and will include the HTML email signature, preserving the email signature formatting.

☑ **Add random disclaimer/signature**: This option will rotate your disclaimers and signatures by randomly adding any disclaimer or signature template that exists in the selected folder. For instance if your company would like to alternate between two different banners, you can save the two banners in a templates folder. Then in Policy Actions, select the option **Add random disclaimer/signature** and select the templates folder where both banners are located. Policy Patrol will randomly insert one of the banners into each email signature. The rest of the options are the same as for the action 'Add disclaimer/signature' as described above.



☑ **Replace word/phrase in subject**: Select this option to replace a word or phrase in the subject. Enter the words or phrases to be replaced in the 'Find' 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. If you tick the case sensitive option, Policy Patrol will only replace the words if they are in the same case as entered in the 'Find' column.

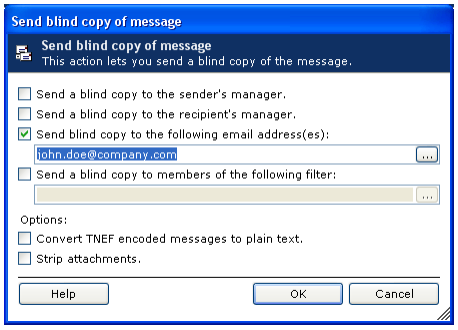
Note: this action is only required if you are adding a vCard to the message and only wish the vCard to be added/suppressed if a code is found in the subject. If you wish to add/suppress a disclaimer/signature if a code is found in the subject, this can be configured form the **Add disclaimer/signature** dialog.



☑ **Attach 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.

- **Message duplication**

☑ **Send blind copy of message**: 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. To send a blind copy to an email address, select **Send blind copy to the following email address(es)** 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. If you wish to enter multiple addresses they must be separated by a semi colon. You can also send a copy to the sender's or recipient's manager, or send a copy to recipients in a filter.



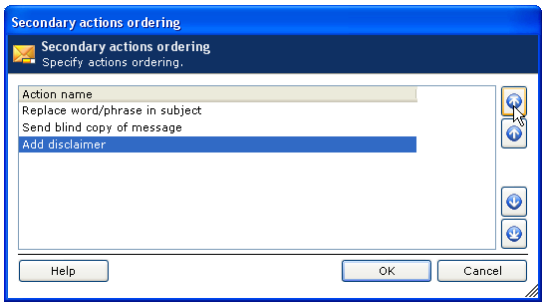
Note

If you want to send a copy of an internal message to an external recipient, you must tick the option **Convert TNEF encoded messages 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.

If you do not want to include attachments in the blind copy, check the option **Strip attachments**.

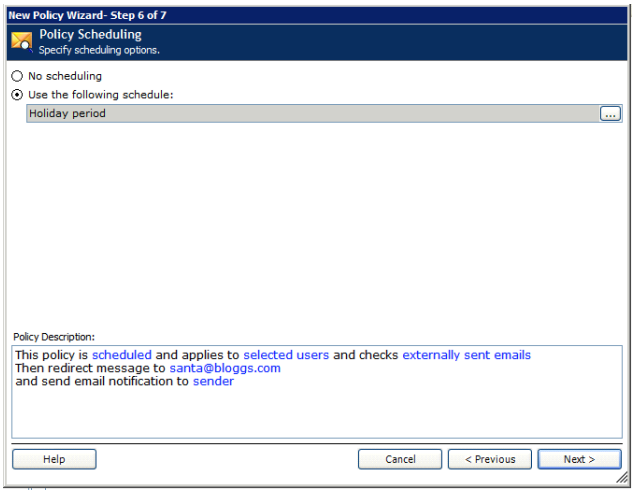
9.1.5.3 Ordering of Secondary Actions

By default Policy Patrol will apply the secondary actions in random order. However, sometimes it can be important that the actions are applied in a certain order. For instance if you want your blind copy to include the disclaimer, the 'Add disclaimer/signature' action must be ordered above the 'Send blind copy' action. To change the order of the secondary actions, click on **Order...**. Then select the action and press the **Move up** or **Move down** buttons.



9.1.6 Step 6. Policy Scheduling

A policy can be scheduled to run on certain days, times, and dates. If you do not wish to schedule the policy, select **No scheduling** and click **Next**. If you wish to schedule the policy, select **Use the following schedule** and select the schedule from the drop down list by clicking on the **...** button. If you wish to create a new schedule, click **New**. For more information on how to create schedules, please consult the paragraph 18.3. 'Schedules'.

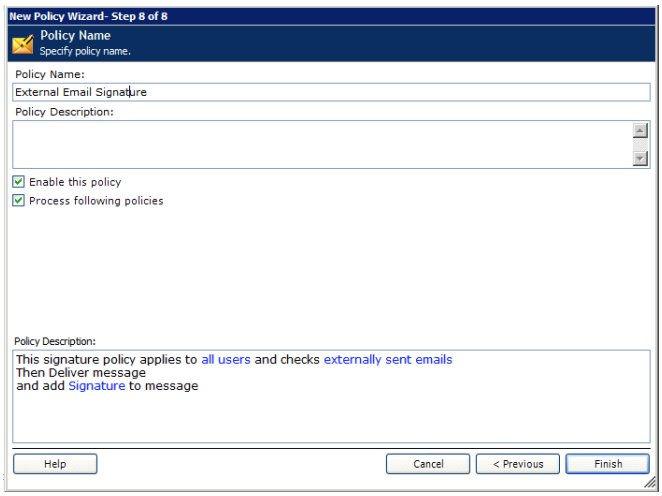


Tip

It can be useful to schedule a policy if for instance you wish to temporarily add a seasonal message to outgoing emails.

9.1.7 Step 7. Policy Name

In the final step, enter a name for the policy and any comments. Uncheck **Enable this policy** if you do not want the policy to be enabled right away. If you do not want any following policies to be processed once this policy has triggered, uncheck the option **Process following policies**. Click **Finish** to create the policy.



9.2 Editing Existing Policies

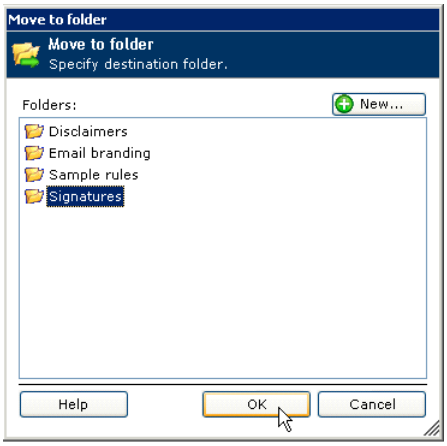
To edit an existing policy, go to **Email Signatures** and select the policy to be edited. Double-click on the policy or click on the **Edit** button. A dialog with several tabs will appear. Make the changes in the appropriate tabs. If you want to change the name of a policy, right-click the policy in the list and select **Rename**. If you want to move a policy to another folder, right-click the policy and select **Move**. Select the folder you wish to move the policy to and click **OK**.

9.3 Copying Policies

To copy an existing policy, right-click the policy and select **Duplicate**. The policy will now be duplicated. The name will be displayed as follows: Copy of <original policy name>.

9.4 Moving Policies

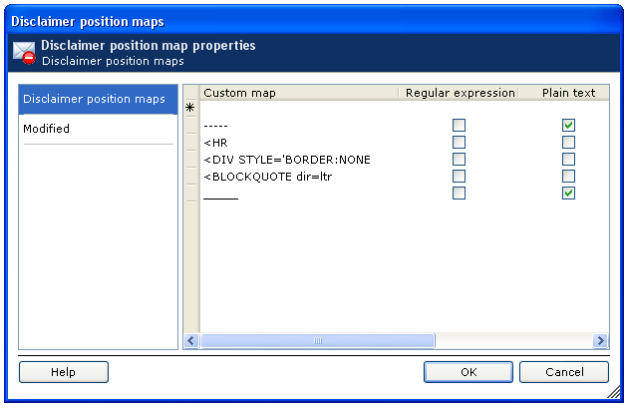
To move a policy to a different folder, right click on the policy and select **Move**. Select the folder you wish to move the policy to and click **OK**. To create a new folder, click the **New...** button.



9.5 Signature Position Maps

For the correct positioning of signatures & disclaimers Policy Patrol makes use of custom positioning maps. If the option **Place after most recent message (recommended for signatures)** is selected in the signature policy, Policy Patrol will search for all the signature position maps and if it finds one it will place it directly above it. These position maps are also used to determine the separators between the 'New Email Body' and 'Previous Email Body' merge fields used in Stationery templates.

Normally you do not need to make changes to the position maps since they are already preconfigured with the most common message separators. If you do want to enter a position map, enter the separator and select whether it is a regular expression. Check the Plain text box if this separator only applies to plain text messages.



9.6 Viewing Signatures in Outlook Sent Items

Policy Patrol can automatically update the emails in Outlook Sent Items to include any email modifications that Policy Patrol might have applied to the email, including adding disclaimers and signatures. The advantages of updating Outlook Sent Items are as follows:

- Obtain proof that your disclaimer was added
- View the formatting of your signature
- Your email archive will contain the actual email that was sent or received

For more information on how to configure this, please consult paragraph 20.3.3 Email Modifications.

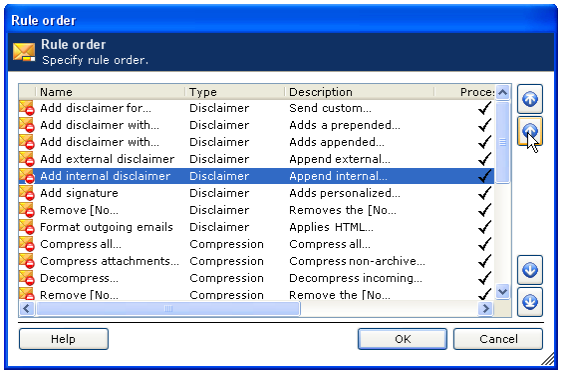
Chapter 10

How to Order Policies

Rules can be ordered to produce a desired result or to optimize processing in Policy Patrol. This chapter discussed how you can order policies.

10.1 Ordering Policies

Policy Patrol allows you to order policies and select whether you wish to continue processing the following policies. To order policies, go to **Email Content Policies** > **Policy Ordering**. Select the policy in the list and press the **Move up** or **Move down** button. To move a policy to the top of the list, press the **Move to the top** button. To move a policy to the bottom of the list, press the **Move to bottom** button.



The order of policies can be important for efficiency reasons and for determining how messages should be processed.

10.1.1 Processing Speed

The way in which policies 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 policies above slow policies. Furthermore, if you have a policy that deletes the message, it is better to order this policy to be processed first, since there is no use for an earlier policy to add a disclaimer or compress an attachment if it is deleted afterwards.

To help you order policies efficiently, consider the speed of the policy by checking the following:

- Is the policy user-based? A user-based policy is slower to process than a global policy. 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 policy 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.

- 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.

10.1.2 Ordering Result

In addition to processing speed, it is also important to order the policies in such a way that the result is correct. For instance when adding multiple disclaimers, the order of the policies will determine the order in which the disclaimers are added to the message (see note below). Another example is a configuration with a policy that prints all mails and another policy 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 policy above the print policy, since otherwise the printed messages will not include the disclaimer.

Note

When ordering disclaimer and tag policies, the consecutive disclaimers or tags will be added as specified below. If you have two prepend disclaimer policies 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 policies, they will be applied as follows:

`Append Disclaimer 1`

`Append Disclaimer 2`

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

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

10.1.3 Process Next Policies

For each policy you can specify whether Policy Patrol must continue to process the next policy. For instance, say you have a policy 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 decides that the mail is legitimate and delivers the message out of quarantine. If you did not select **Process following policies** in the quarantine policy (or the Administrator did not select to **Process any remaining policies** when delivering the message out of quarantine), the message would be delivered regardless of the 6 MB attachment. If you selected to process the following policy (in the policy or when delivering the message), then Policy Patrol will consequently delay the message for delivery at the specified time. However, this might sometimes produce unwanted results if another policy quarantines the same message again. Therefore if any policies always need to be applied, you must order these policies above the quarantine policy. In that way, all necessary policies will be applied and no messages will be quarantined multiple times.

Chapter 11

Creating Filters

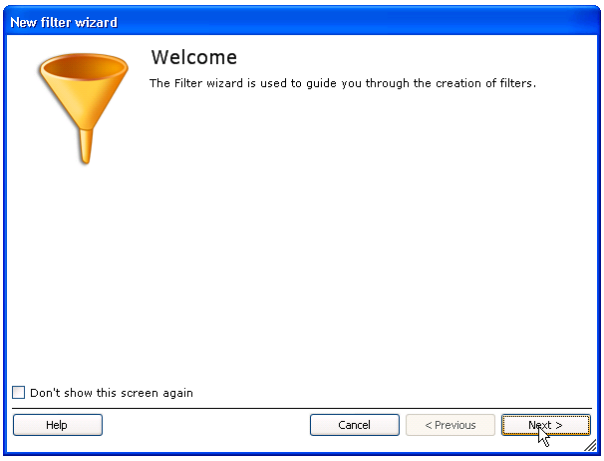
Filters are lists that Policy Patrol must check for. Policy Patrol includes Word/phrase, Attachment and Email/domain filters. This chapter explains how to create each type of Policy Patrol filter.

11.1 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 filters. To create your own Word/phrase filter:

1. Go to **Settings** > **Filters**, select the appropriate folder and click **New...**.

2. Click **Next** in the Welcome screen.



3. When asked which type of filter you wish to create, select **Word/Phrase Filter**. Click **Next**.

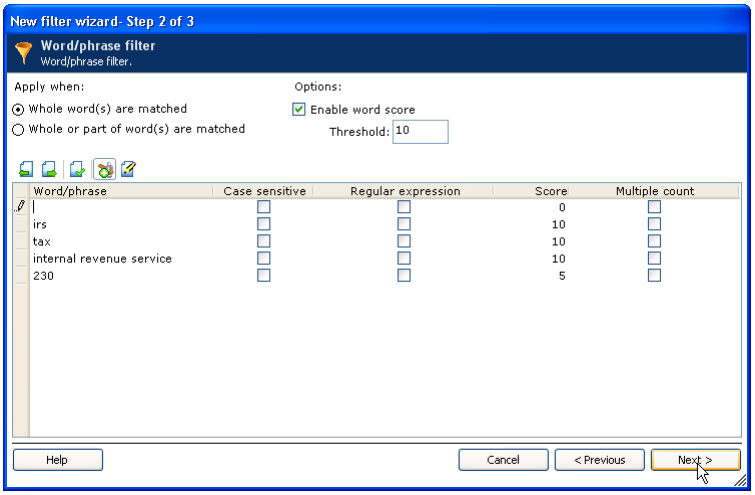
4. Enter the word(s) or phrases to be included in the filter. The following options are available:

   Case Sensitivity

   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.

Regular Expression

If the entry is a regular expression tick the box **Regular Expression**. Regular expressions allow you to match a word pattern instead of an exact word. This means that by making use of regular expressions you can stop spammers trying to circumvent content filters by adding characters within words, such as v*i*a*g*r*a or c-l-i-c-k h-e-r-e. Furthermore you can detect word variations such as r@tes and l0ans.

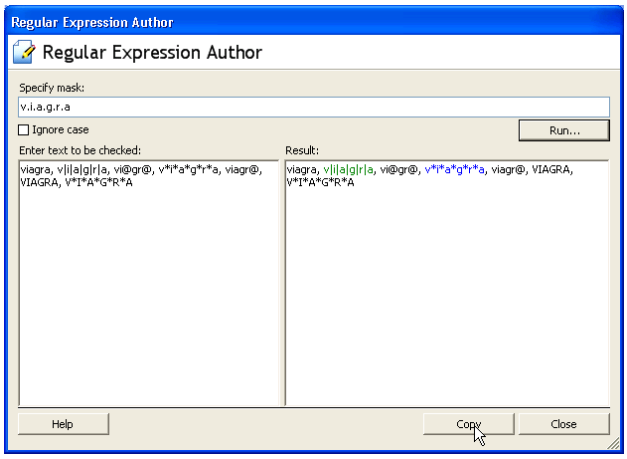


Note

Be cautious when using the * sign in word entries. If the word is not marked as a regular expression, the * is seen as a wildcard for any character. This means that if you enter the word v*i*a*g*r*a this will not only find v/i/a/g/r/a and v-i-a-g-r-a, but also the phrase: Victor is a great person. If you enter the word v*i*a*g*r*a and check the regular expression tick box, this means that the entry will trigger on all words since the * sign means 0 or more of the previous character.

Policy Patrol includes a Regular Expression Author to help you create and test your regular expressions. Follow the next steps to use the Regular Expression Author:

1. Click on the **Regular Expression Author** icon in the toolbar .



2. In **Mask**, enter your regular expression, for instance `v.i.a.g.r.a`. If you wish to ignore case, select the option **Ignore Case**.

3. In the left dialog, enter the sample text to be checked for the regular expression.

4. Click on **Run**. The words that match the regular expression will be colored green and blue alternately. For instance, in the example above, you can see that the regular expression v.i.a.g.r.a matches v*i*a*g*r*a, but not viagra or vi@gr@.

5. If the result is not as you had intended, alter the regular expression and press **Run** again. If your regular expression produced the intended results, press **Copy** and **Close**. Now paste the regular expression into the word/phrase filter and tick the box **Regular Expression**.

Note

The options **Whole word(s) are matched** and **Whole or part of word(s) are matched** do not apply to regular expressions since this can be indicated in the regular expression itself.

More information about regular expressions can be found in the following document:

Using Regular Expressions in Policy Patrol
(http://www.policypatrol.com/assets/pp10-regularexpressions.pdf)

Word Score

If you want to use word score, you must apply a score for each individual word and a total word score threshold for the filter. If the message body or subject reaches the word score threshold, the policy will trigger. You can also apply a negative word score for a word. 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. If you do not wish to use word score in the filter, uncheck **Enable word score**. More information about word/phrase filtering can be found in the following document:

 How to configure word/phrase filtering
(http://www.policypatrol.com/assets/pp10-wordfiltering.pdf)

Multiple Count

If you wish every instance of the word to be counted, check the box **Multiple Count**. For example, if this box is enabled and you receive an email message that contains the word 'debt' three times, and you applied word score of 5 to this word, the total word score would be 15. If you did not check this box, the word will only be counted once and the total score would be 5.

Whole words/part of words

You can 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 policy. 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 policy will trigger on the word 'sex' but not on 'Middlesex'.

Import/Export

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[TAB]Case sensitive[TAB]Regular expression[TAB]Score[TAB]Multiple count. The word/phrase and score values must be entered. For the other options, either 1 (enabled) or 0 (disabled) must be entered. For instance, if you wish to add the case sensitive word CLICK HERE with a word score of 5 and multiple count, you must enter it in the text file as follows: `CLICK HERE 1 0 5 1`. For every word or phrase you need to start a new line. To export the words in the filter, click **Export**, enter a file name and select **OK**.

Remove Duplicates

If you wish to remove duplicates in the filter, click on the remove duplicates button in the toolbar.

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

5. Enter a name for the filter and a description. When you are done, click **Finish** to create the filter.

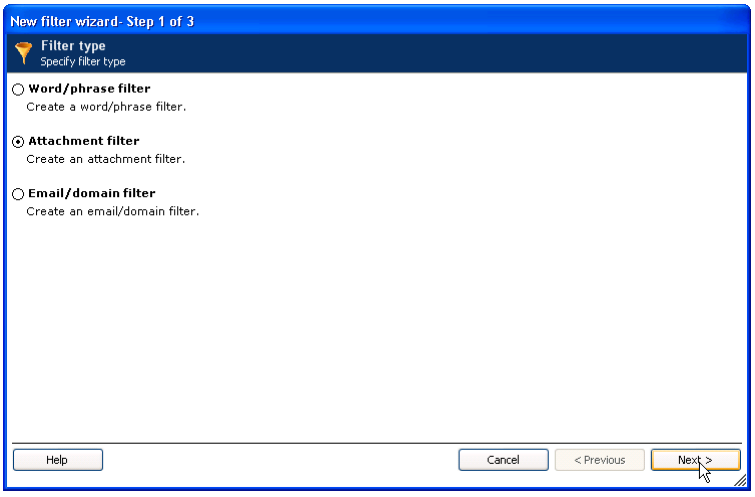
11.2 Creating an Attachment Filter

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

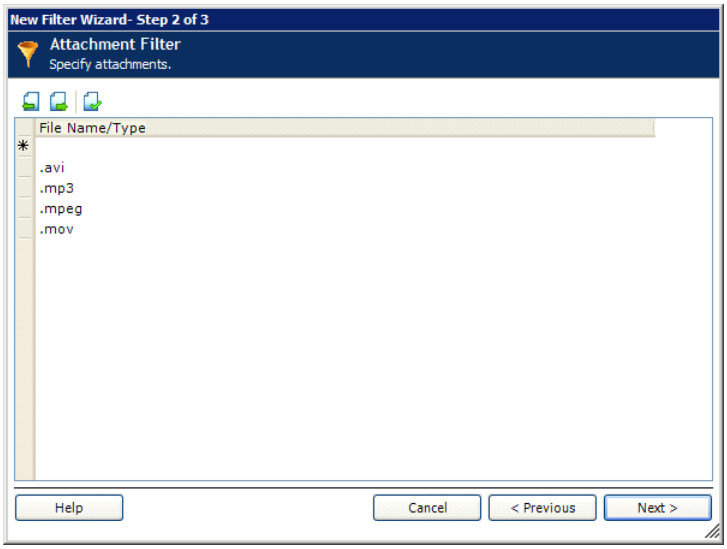
1. Go to **Settings** > **Filters**, select the appropriate folder and click **New...**.

2. Click **Next** in the Welcome screen.

3. When asked which type of filter you wish to create, select **Attachment Filter**. Click **Next**.



4. Enter the attachment names or extensions for the filter. You can choose to enter an extension, the exact file name or only enter a word that must be found in the file name. When entering the data you can make use of the wildcards * and ?, where * stands for any amount of characters and ? stands for one character. To enter an extension, enter the part after the period (no need to place a * in front of the extension), .e.g `.exe` for executable files. If you wish to search for file names no matter which extension they have, enter the name followed by .*, e.g. `readme.*`. This will find the files readme.exe, readme.doc and readme.txt. If you want to search for files that include a certain word, you can do so by entering the word in between *. For instance, if you enter `*price*` in the filter, this will apply to the files pricelist.doc and ukpricelist.htm. Note that the entries 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 entry should be on a separate line. To export the entries click **Export**, enter a file name and select **OK**. If you want to remove double entries in the filter, click on **Remove duplicates**. When you are ready adding attachment names and extensions, click **Next**.

5. Enter a name for the filter and a description. When you are done, click **Finish** to create the filter.

11.3 Creating an Email/Domain Filter

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

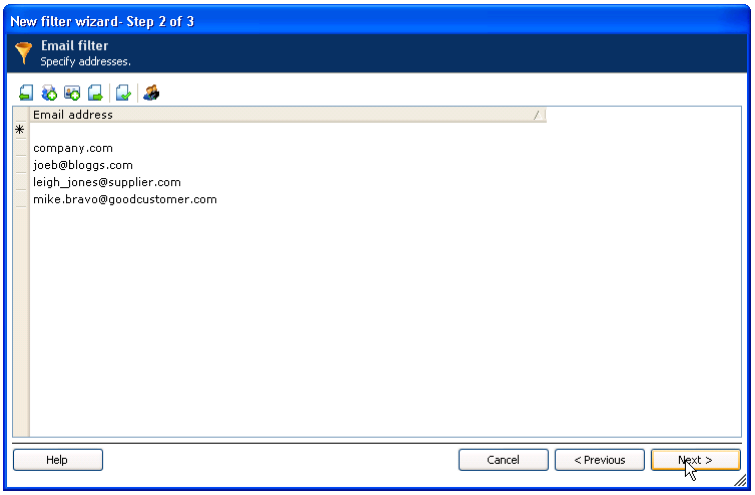
1. Go to **Settings** > **Filters**, select the appropriate folder and click **New...**.

2. In the Welcome screen, click **Next**.

3. When asked which type of filter you wish to create, select **Email/Domain Filter**. Click **Next**.

4. Enter the email addresses or domains in the list. You can either enter a complete email address, or enter a domain e.g. `domain.com`. This will include all email addresses ending in @domain.com, for instance JohnD@domain.com. If you enter `*domain.com` this will include email addresses such as JohnD@domain.com, but also JohnD@test.domain.com and JohnDoe@salesdomain.com. If you enter `company.*` this will include all domains starting with company, for instance company.com and company.co.uk, but not sales.company.com. You can also enter a word that must be found in the email address, such as `*free*`. This will include domains such as freemail.com and spam-free.com, but also email addresses such as free@company.com. Try to only use wild cards when necessary since they can be a burden on performance.

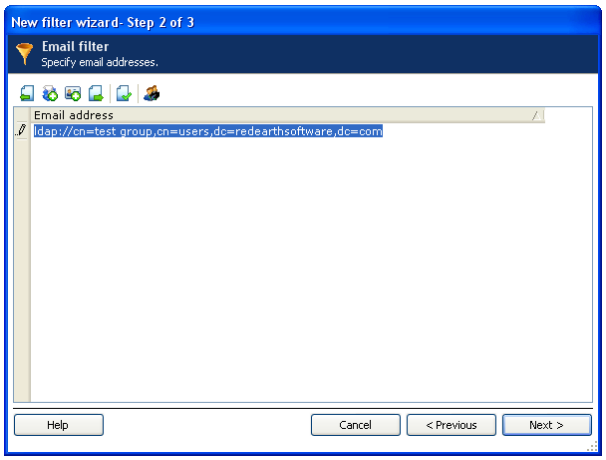
   You can import lists from .txt files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. In the text file to import, each domain/email address should be entered on a separate line. To export the filter, click **Export**, enter a file name and select **OK**. If you want to remove double entries in the filter, click on **Remove duplicates**. To sort email addresses on domain, click on the **Group by email domain** button in the tool bar. When you are ready, click **Next**.



5. Enter a name for the filter and a description. When you are done, click **Finish** to create the filter.

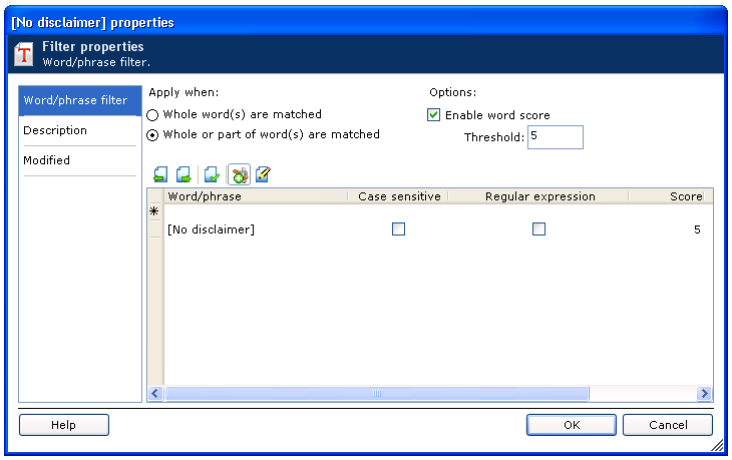
11.3.1 Active Directory Users in Email Filter

In order to apply policies to specific internal email traffic from one group to another, you need to select the users for the policy and select the Active Directory users in the Recipient condition too. To do this, you can create an Email/domain filter that contains an LDAP query instead of an email address. In step 4 above, enter the Active Directory path for the user or group, for example: ldap://cn=test group,cn=users,dc=redearthsoftware,dc=com. Then select this filter in the **Recipient address exists in filter** condition of the policy. Note that the total length of the path must not exceed 100 characters.



11.4 Editing Filters

To edit an existing filter, select the filter and click **Edit**. A tabbed dialog will now appear. You will be able to add or delete entries and change the description for the filter. The Modified tab includes information on when the filter was created and by whom. It also includes information on when the filter was last modified.



You can change the filter name by right-clicking on the filter in the list and selecting **Rename**. To move a filter to a different folder, right-click on the filter and select **Move**. Select the folder to move the filter to and click **OK**.

> **Note**
>
> If you rename a filter that has already been configured for a policy, the policy 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 policy properties and open the dialog where the filter is selected. Click **OK** to save the new name in the policy.

11.5 Copying Filters

To copy an existing filter, right-click the filter and select **Duplicate**. The filter will now be duplicated. The name will be displayed as follows: Copy of <original filter name>.

11.6 Moving Filters

To move an existing filter, right-click the filter and select **Move**. Select the folder you wish to move the filter to and click **OK**. To create a new folder, click the **New...** button.

11.7 Content Checking Attachments

Note that by default Policy Patrol can only content check .txt file and .html file attachments. If you wish Policy Patrol to content check other attachment types such as Microsoft Word or PDF files, you must install the appropriate IFilters on the Policy Patrol machine. IFilters can be downloaded from the following web pages:

- Microsoft Office: http://www.microsoft.com/downloads/details.aspx?FamilyId=60C92A37-719C-4077-B5C6-CAC34F4227CC&displaylang=en.
- Pdf: http://www.adobe.com/support/downloads/detail.jsp?ftpID=2611 (32-bit) and http://www.adobe.com/support/downloads/detail.jsp?ftpID=4025 (64-bit)
- Other IFilters: http://www.ifilter.org/Links.htm

Chapter 12

Creating Templates

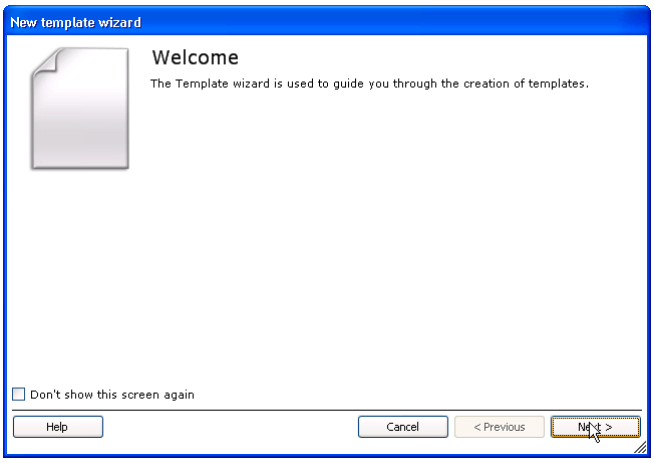
Templates are pre-configured texts that can be used in Policy Patrol. This chapter describes how to create notification, tag and disclaimer templates.

12.1 Creating an Email Notification Template

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

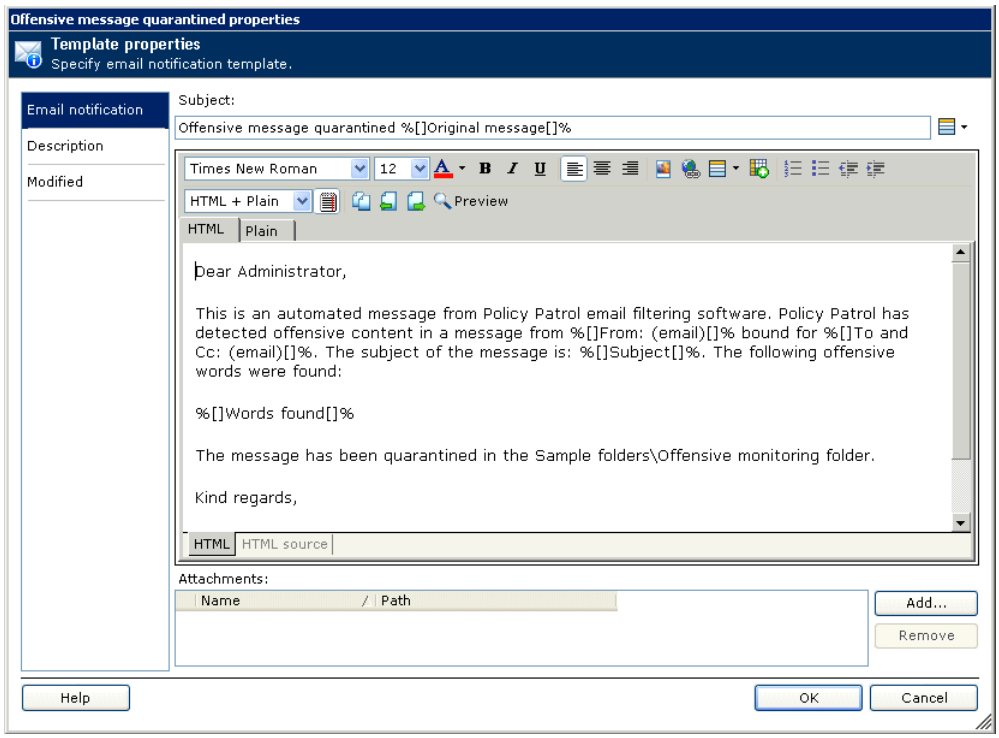
1. Go to **Settings** > **Templates**, select the appropriate folder and click **New...**.

2. In the Welcome screen, click **Next**.



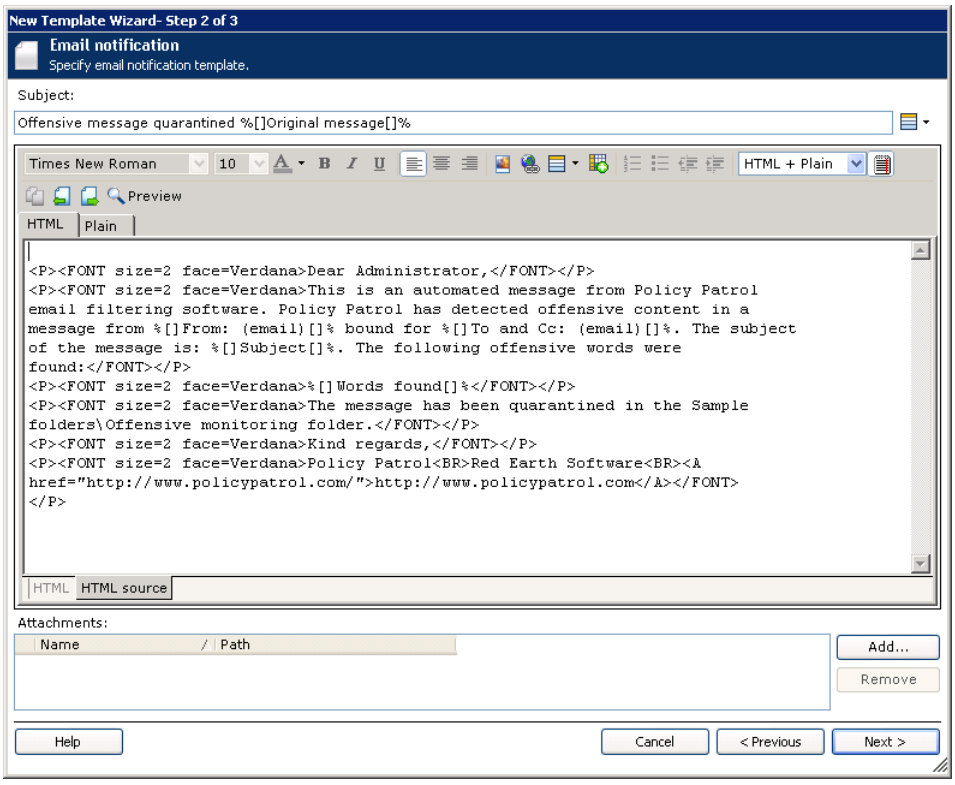
3. When asked which type of template you wish to create, select **Email Notification Template**. Click **Next**.

4. Enter the subject for the notification email. You can include fields in the subject by clicking on the **Insert Field** button to the right of 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. By default, the option **HTML + Plain** is selected. Leave this selected if you are not sure whether the recipient can read HTML messages. Although nowadays most clients can read HTML, there are some clients on for instance mobile devices 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.

In the HTML tab you can directly edit the HTML source by clicking on **HTML Source** at the bottom of the dialog, for instance to add tables or bullets. If you wish to clean up the HTML, click on the **Clean HTML** button in the toolbar.



Note

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

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.

Note

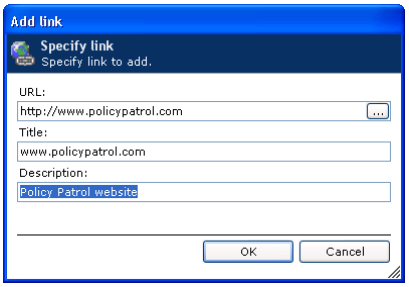
Note that if you enter the Original message field it is best to enter it in the subject since if you add it to the body of the HTML as well as the Plain text tab, the message will be added twice.

Tip

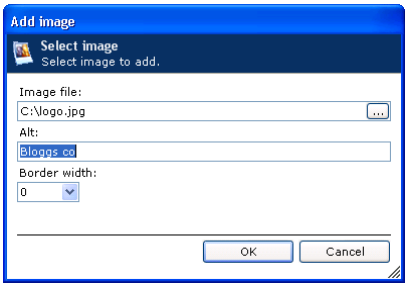
It is possible to manipulate Active Directory merge fields so that if not all users have the same Active Directory information, certain fields will not be shown for all users. For instance if some users do not have a cell phone number in their Active Directory properties, these fields can be hidden for those users without a cell phone number. For

more information on how to configure this, consult the paragraph 12.11 'Inserting AD fields depending on user's AD information'.

The text can be formatted by selecting font type, size or color and applying bold, italicized or underlined styles. To add a link, click on the **Insert Link** button. In **URL:** enter the URL to link to. Enter the text to be displayed in **Title** and enter the description in **Description**.



You can insert gif and jpeg pictures by clicking on the **Insert Image** button. In **Image File**, enter the path to the picture. Note that this picture must be located on the local drive. Alternatively you can enter the URL of an image on a website. Note: If you are using Policy Patrol for Exchange 2007/2010/2013 64-bit, it is advisable to store the image within the Policy Patrol installation folder to ensure that Policy Patrol has the necessary permissions to access the file. In **Alt**, enter the text that you wish to appear as a tool tip. If you want a border to be applied to the image, set a border width.



To add an attachment to the notification, click on **Add...**. Enter the file name and click **OK**. Note that the file must be located on the local drive. If you are using Policy Patrol for Exchange 2007, it is advisable to store the image within the Policy Patrol installation folder to ensure that Policy Patrol has the necessary permissions to access the file.

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**.

5. Enter the template name and a description. Click **Finish** to create the template.

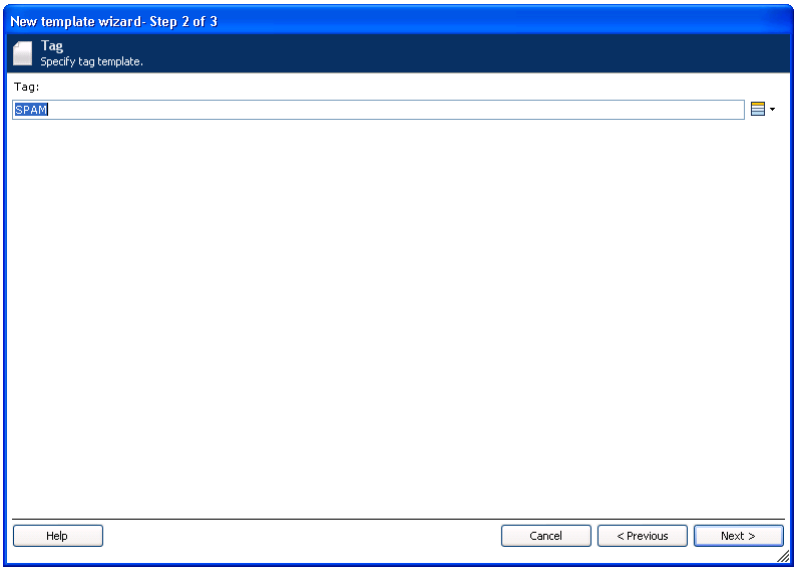
12.2 Creating a Tag Template

Tags can be added to an email subject and are used for network messages. 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**, select the appropriate folder 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 button **Insert Field** . For more information on the available fields, see the 'Fields' paragraph. Click **Next**.



4. Enter the template name and a description. Click **Finish** to create the template.

12.3 Creating a Disclaimer/Signature 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. There are two types of Disclaimer templates:

Standard Disclaimer/Signature Template: This template is used to add a block of text to the top or bottom of an email (or below the last message text). This text can be formatted and include pictures, but it does not alter the actual email message text. It is simply added below or above the existing message text.

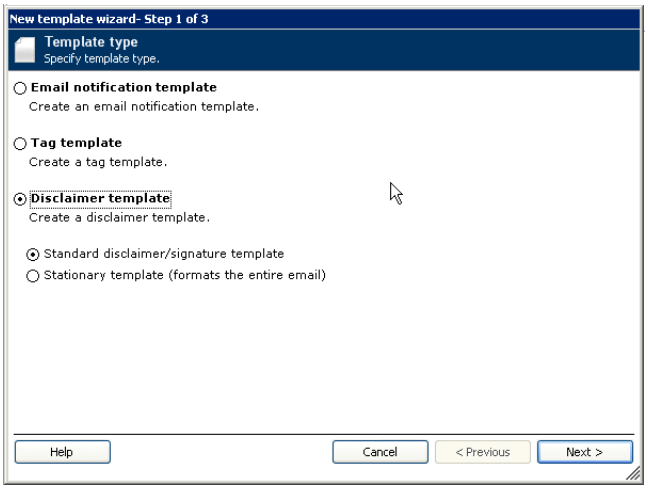
Stationery Template (formats the entire email): This template is used if you wish to add a disclaimer or signature and format the entire email, including the original body text. For instance if you wanted to format your emails like a web page, or you want to add your contact details in a column to the right of your email message, you can use the Stationery template to do this.

12.3.1 Creating a Standard Disclaimer/Signature Template

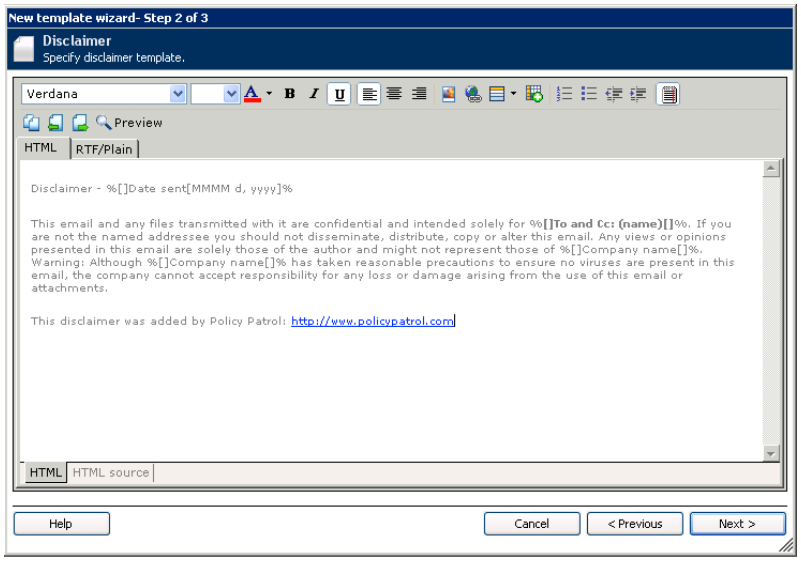
To create a standard Disclaimer/Signature template:

1. Go to **Templates**, select the appropriate folder and click **New...**.

2. When asked which type of template you wish to create, select **Signature Template > Standard Disclaimer/Signature template**.



3. 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. 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. To copy text from the HTML tab to the RTF/Plain tab (or vice versa), click on the button **Copy to..** .

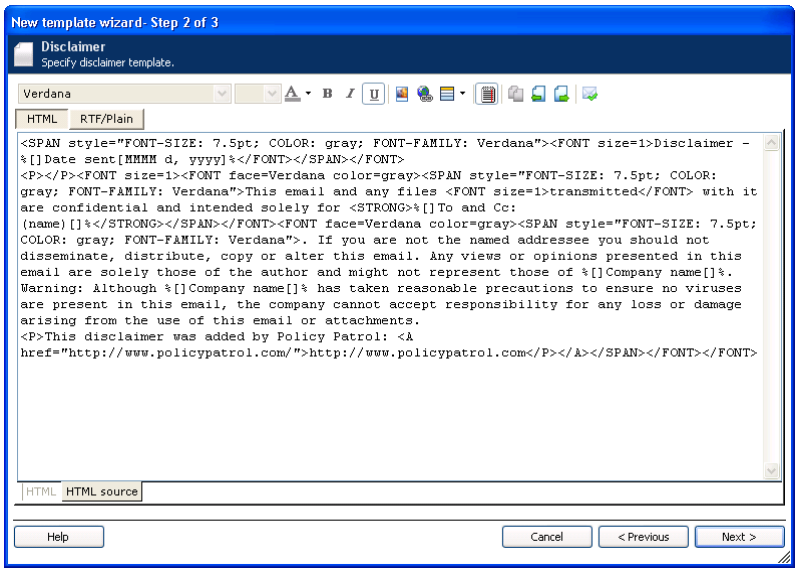


Note

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

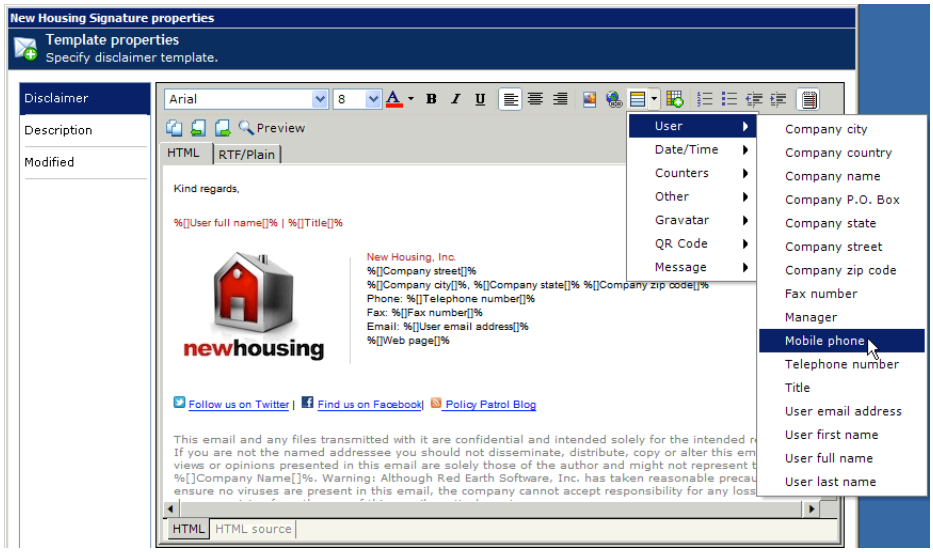
must always enter a disclaimer text in the RTF/plain text tab, even if you only send out HTML messages. However, you only need to enter your text once, since you can copy and paste the text from one tab to another by clicking on the **Copy to..** button.

In the HTML tab you can directly edit the HTML source by clicking on **HTML Source** at the bottom of the dialog, for instance to add tables or bullets.

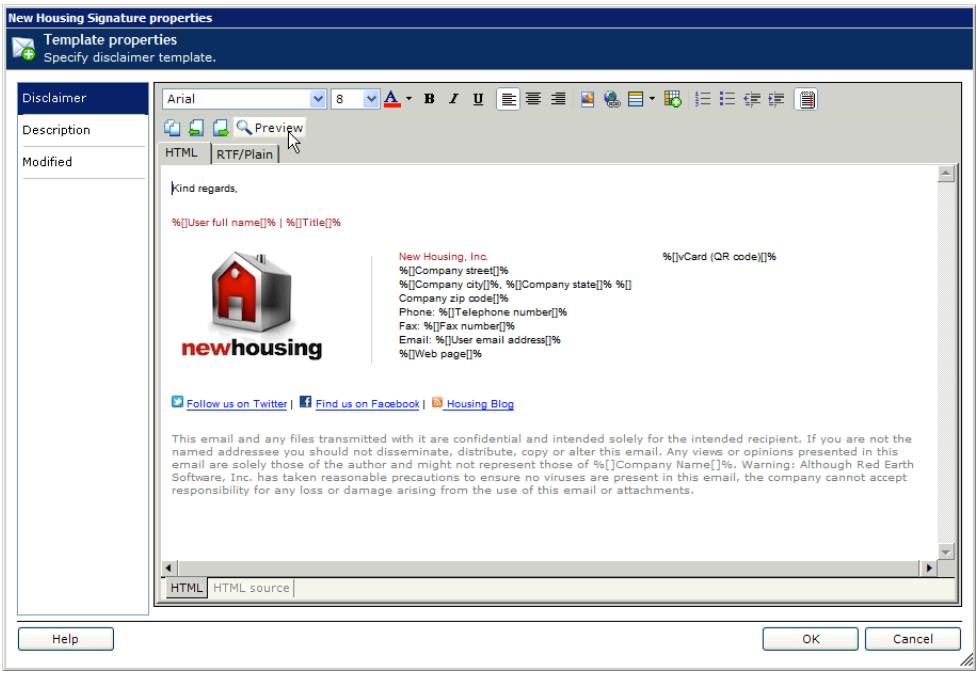


From the toolbar, you can select font, size, color, bold, italic, and underlined. You can add bulleted lists, numbered lists, indent and align text.

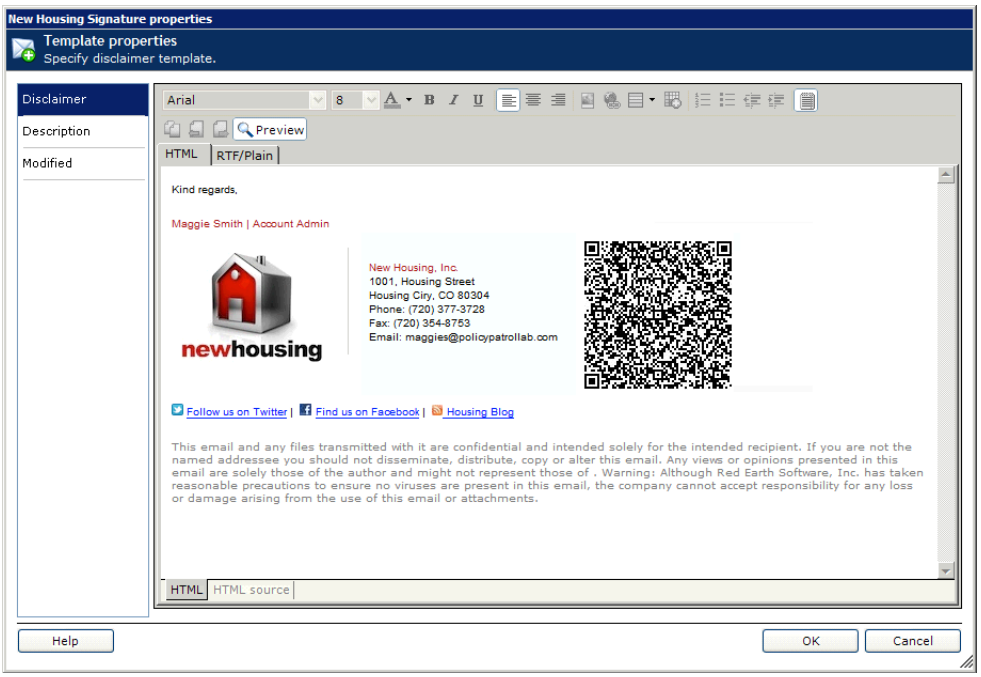
You can insert merge fields by clicking on the **Insert Field** icon and selecting the relevant field. For more information on the available fields, see the 'Fields' paragraph in this chapter.



If you are using fields in your disclaimer or signature, Policy Patrol includes a preview option so that you can check whether the merge fields will be replaced correctly. To see the preview, click on the **Preview** icon in the toolbar.



A dialog will pop up asking you to select a user. Select a user and click **OK**. You will now see the disclaimer/signature with Active Directory merge fields replaced by the Active Directory information for the user. Message fields will be replaced with test data. In case a merge field is still showing in the preview, this means that the field has not been entered correctly. To go back to the normal view, click on the Preview icon again.



Tip

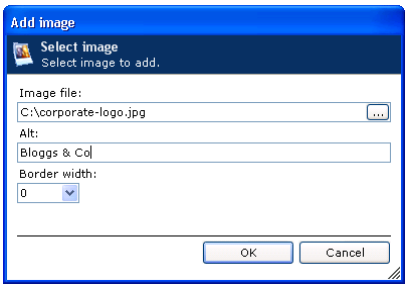
It is possible to manipulate Active Directory merge fields so that if not all users have the same Active Directory information, certain fields will not be shown for all users. For instance if some users do not have a cell phone number in their Active Directory properties, these fields can be hidden for those users without a cell phone number. For more information on how to configure this, consult the paragraph 12.11 'Inserting AD fields depending on user's AD information'.

To send a test email to see what the signature looks like, click on the **Test Email** button. Select a user from the list and click **OK**. The user will now receive a test email with their signature included. Remember however that if you just made changes in the template, that you must first save and close the template and then reopen it for the test email to include the latest changes.

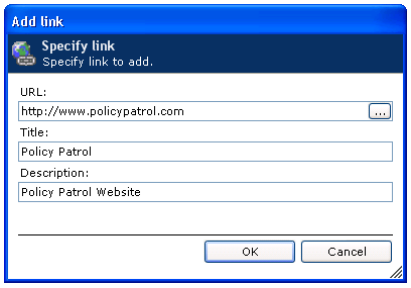
You can import texts from .txt and .html documents by clicking **Import**. Similarly, you can export the text to a .txt or .html file by clicking **Export**.

You can insert gif and jpeg pictures by clicking on the **Insert Image** button. In **Image File**, enter the path to the picture. Note that this picture must be located on the local drive. Alternatively you can enter the URL to an image on a website. In **Alt**, enter the text that you wish to appear as a tool tip. If you want a border to be applied to the image, set a border width.

For instructions on how to insert images or personalized URLs (such as LinkedIn URLs) from Active Directory, please consult paragraph 12.6 'Inserting images and URLs from Active Directory'.

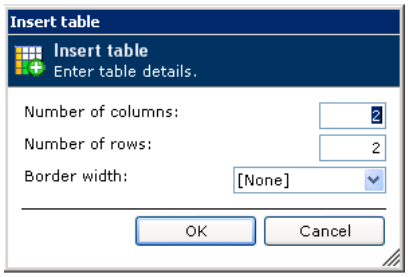


To add a link, click on the **Insert Link** button. In **URL:** enter the URL to link to. Enter the text to be displayed in **Title** and enter the description in **Description**.



You can insert a table by clicking on the **Insert Table** icon in the toolbar. You can select the number of columns and rows and the border width. Tip: Even if you do not intend to show any borders, you can add the Table with a border first, and then later change the border to 0 in the HTML Code (click on HTML Source tab to see the HTML code); For instance if you configured the table to have a border width of 1, you will see `<TABLE style="BORDER-COLLAPSE: collapse" border=1` in the HTML code. When you have finished designing your text and images in the table, change 1 to 0: `<TABLE style="BORDER-COLLAPSE: collapse" border=0`. When you click back on the HTML tab, the table border will be gone.

When you are ready designing your template, click **Next**.



4. Enter the template name and a description. Click **Finish** to create the template.

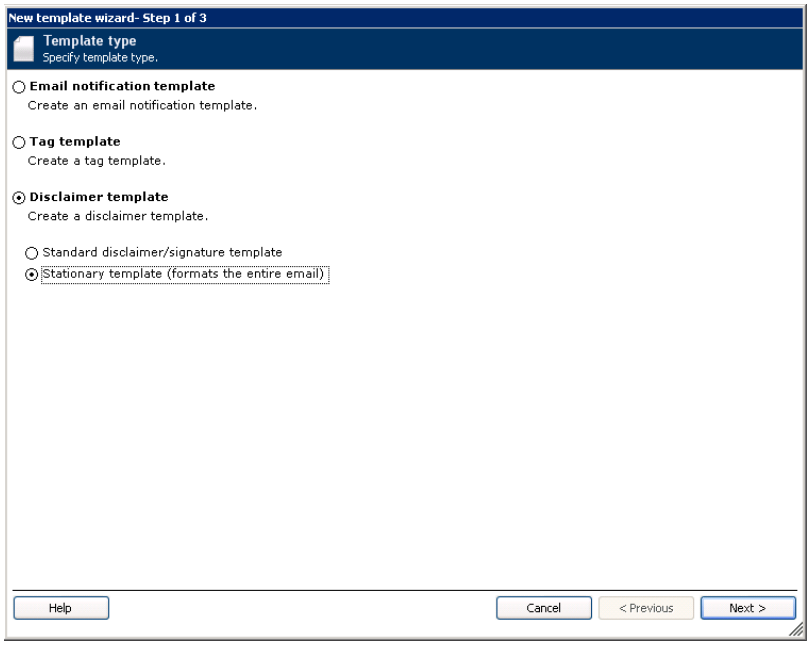
12.3.2 Creating an HTML Stationery Disclaimer Template

The HTML Stationery Disclaimer Template is the same as the standard Disclaimer template, with two exceptions: (1) Stationery templates include two merge fields that will be replaced by the original email body, (2) Stationery templates can only be applied to HTML messages.

To create an HTML Stationery Disclaimer template:

1. Go to **Templates**, select the appropriate folder and click **New...**.

2. When asked which type of template you wish to create, select **Signature template > Stationery Template (formats the entire email)**.



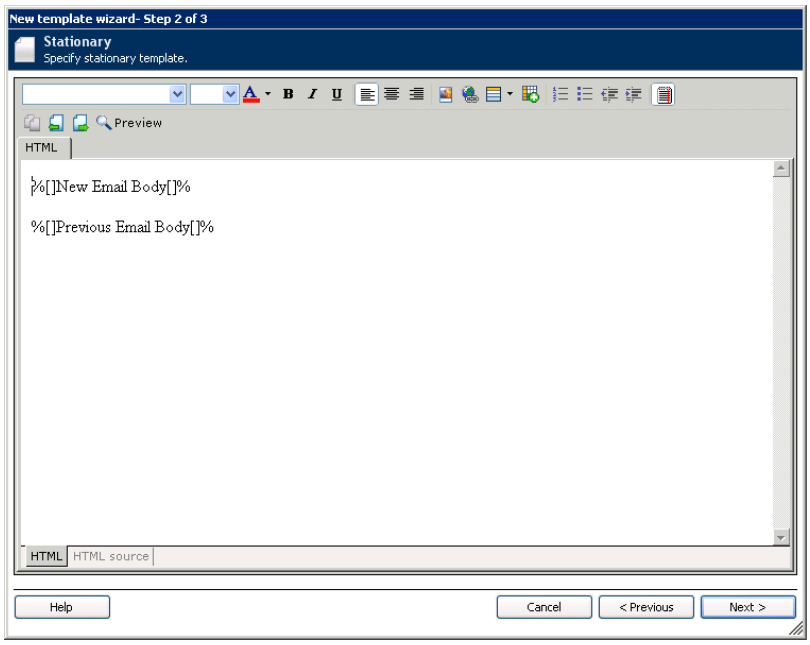
3. You will see two merge fields in the template:

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

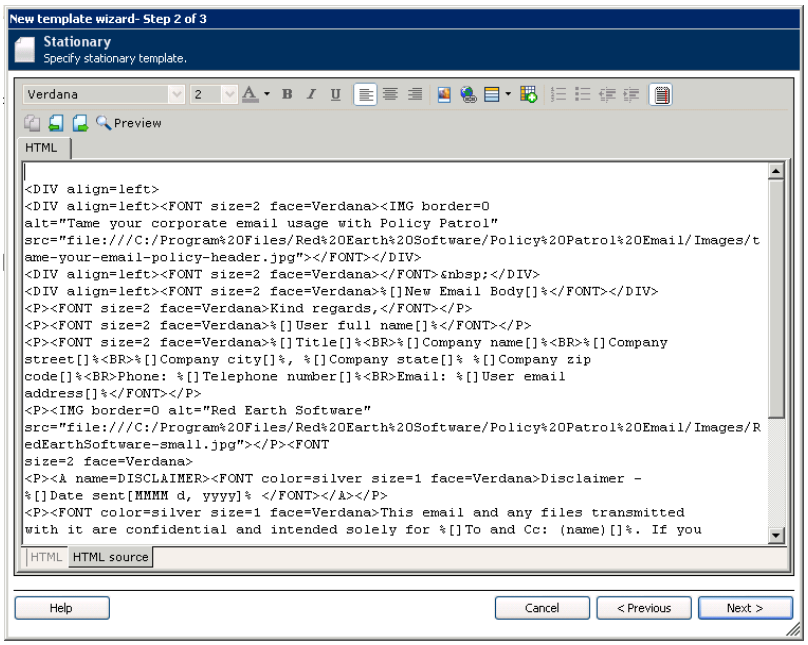
   %[]Previous Email Body[]%:This field will be replaced with the previous message text, i.e. the email text below the first message separator.

   Note that the above merge fields should always be included in the HTML Stationery template.

> **Note**
>
> For a list of message separators, go to **Email Signatures** > **Signature Position Maps**.

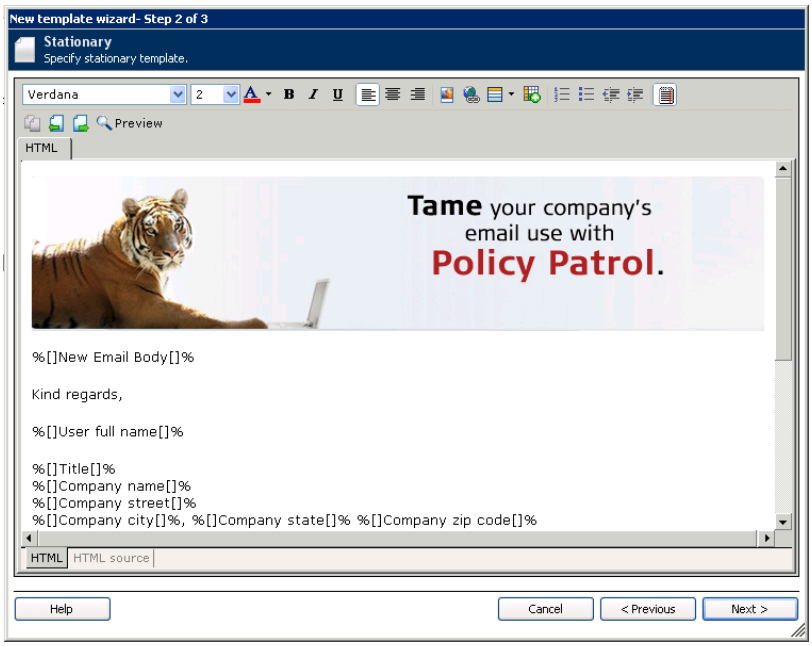


You can directly edit the HTML source by clicking on **HTML Source** at the bottom of the dialog.



From the toolbar, you can select font, size, color, bold, italic, and underlined. You can add bulleted lists, numbered lists, indent and align text.

You can insert merge fields by clicking on the **Insert Field** icon and selecting the relevant field. For more information on the available fields, see the 'Fields' paragraph in this chapter.



Policy Patrol includes a preview option so that you can check whether the merge fields will be replaced correctly. To see the preview, click on the **Preview** icon 🔍 in the toolbar. A dialog will pop up asking you to select a user. Select a user and click **OK**. You will now see the disclaimer/signature with Active Directory merge fields replaced by the Active Directory information for the user. The Message fields will be replaced with test data. In case a merge field is still showing in the preview, this means that the field has not been entered correctly. To go back to the normal view, click on the Preview icon again.

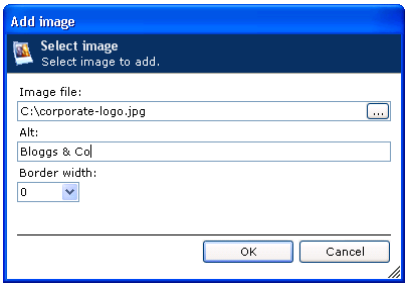
Tip

It is possible to manipulate Active Directory merge fields so that if not all users have the same Active Directory information, certain fields will not be shown for all users. For instance if some users do not have a cell phone number in their Active Directory properties, these fields can be hidden for those users without a cell phone number. For more information on how to configure this, consult the paragraph 12.11 'Inserting AD fields depending on user's AD information'.

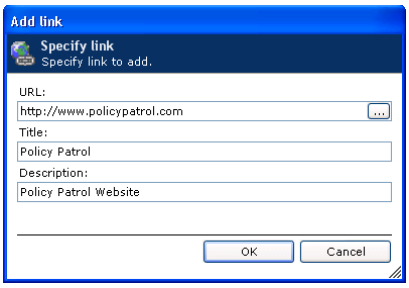
You can import texts from .txt and .html documents by clicking **Import**. Similarly, you can export the text to a .txt or .html file by clicking **Export**.

You can insert gif and jpeg pictures by clicking on the **Insert Image** button. In **Image File**, enter the path to the picture. Note that this picture must be located on the local drive. Alternatively you can enter the URL to an image on a website. In **Alt**, enter the text that you wish to appear as a tool tip. If you want a border to be applied to the image, set a border width.

For instructions on how to insert images or personalized URLs (such as LinkedIn URLs) from Active Directory, please consult paragraph 12.6 'Inserting images and URLs from Active Directory'.

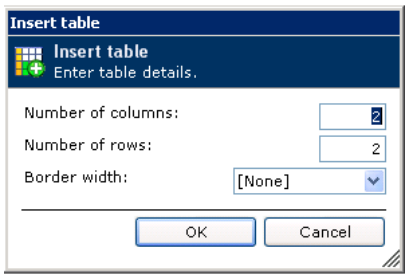


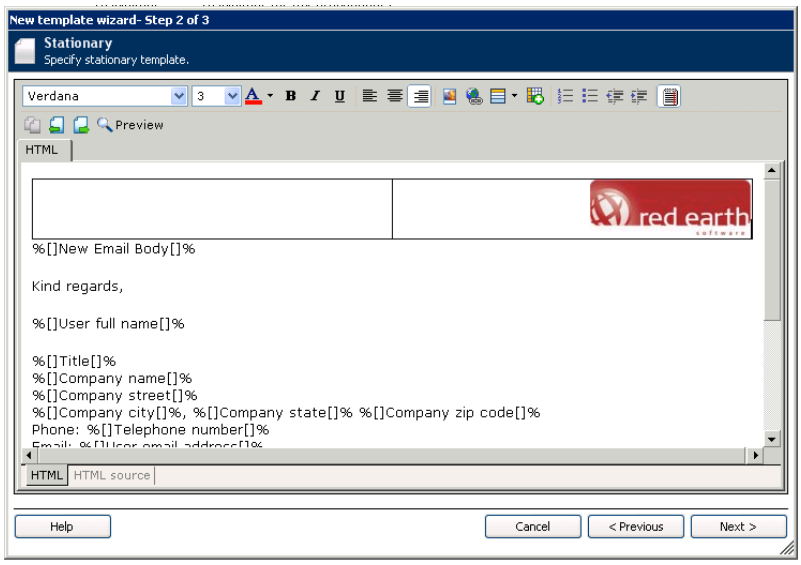
To add a link, click on the **Insert Link** button. In **URL:** enter the URL to link to. Enter the text to be displayed in **Title** and enter the description in **Description**.



You can insert a table by clicking on the **Insert Table** icon in the toolbar. You can select the number of columns and rows and the border width. Tip: Even if you do not intend to show any borders, you can add the Table with a border first, and then later change the border to 0 in the HTML Code (click on HTML Source tab to see the HTML code); For instance if you configured the table to have a border width of 1, you will see `<TABLE style="BORDER-COLLAPSE: collapse" border=1` in the HTML code. When you have finished designing your text and images in the table, change 1 to 0: `<TABLE style="BORDER-COLLAPSE: collapse" border=0`. When you click back on the HTML tab, the table border will be gone.

When you are ready designing your template, click **Next**.



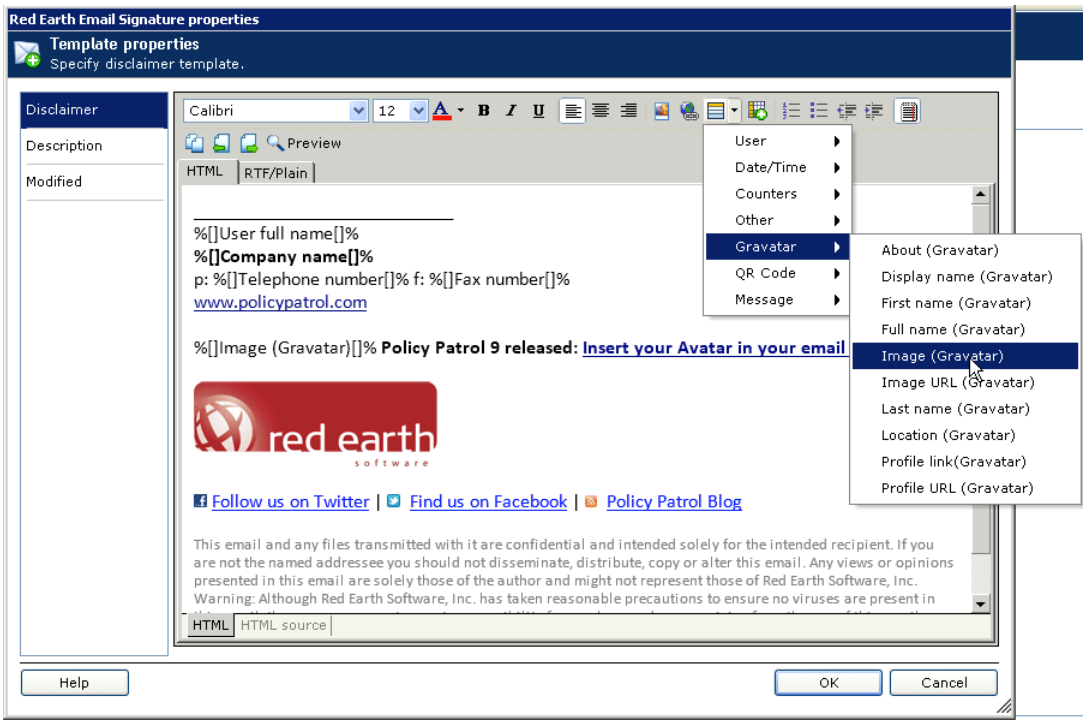


4. Enter the template name and a description. Click **Finish** to create the template.

12.4 Inserting an Avatar in the Email Signature

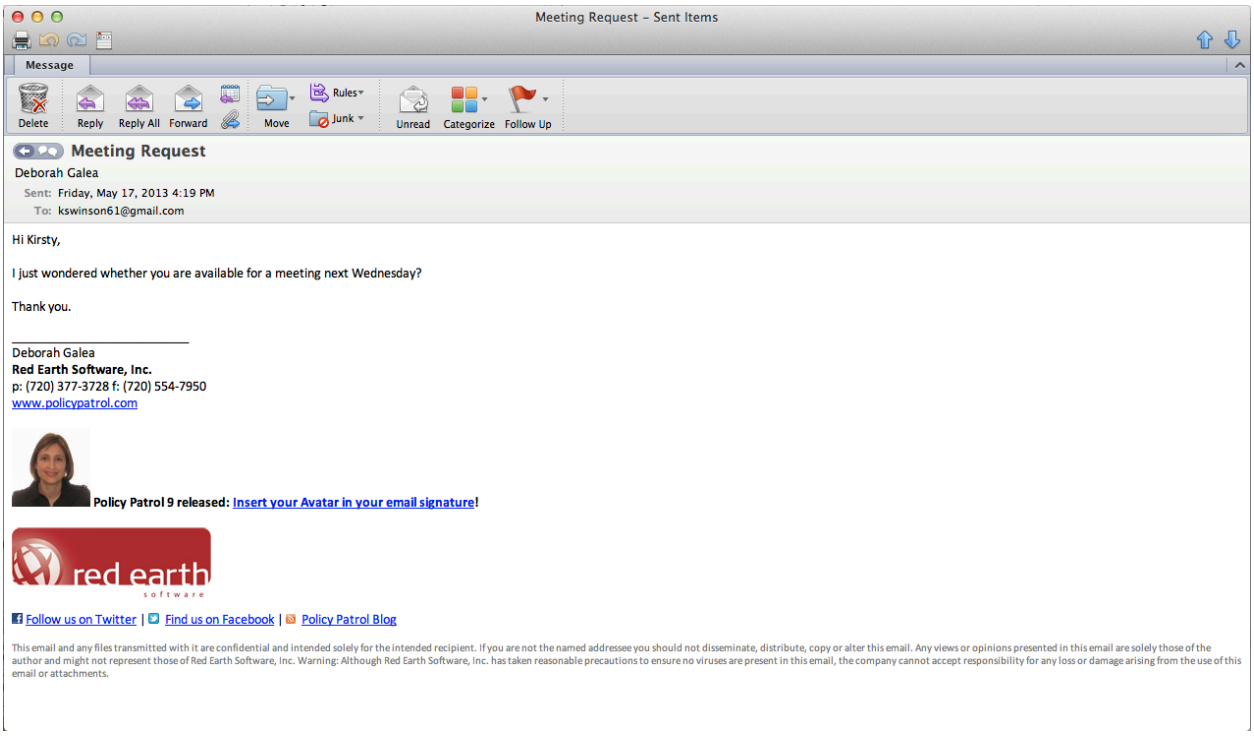
Policy Patrol allows you to automatically insert the sender's thumbnail picture into the email without having to upload and maintain your employees' pictures in Active Directory. Gravatar.com is a free service that stores a user's avatar (thumbnail picture) and then allows programs such as help desks and CRM systems to display the thumbnail for the user. In this way the user only needs to upload their picture in one location, instead of for each program individually. Since the process is intuitive, each user can upload their own picture without any help from IT.

To add the sender's avatar in the email signature, the sender first needs to upload their picture at www.gravatar.com. Then you can insert the avatar merge field in the email signature template by selecting **Insert Field** > **Gravatar** > **Image (Gravatar)**.



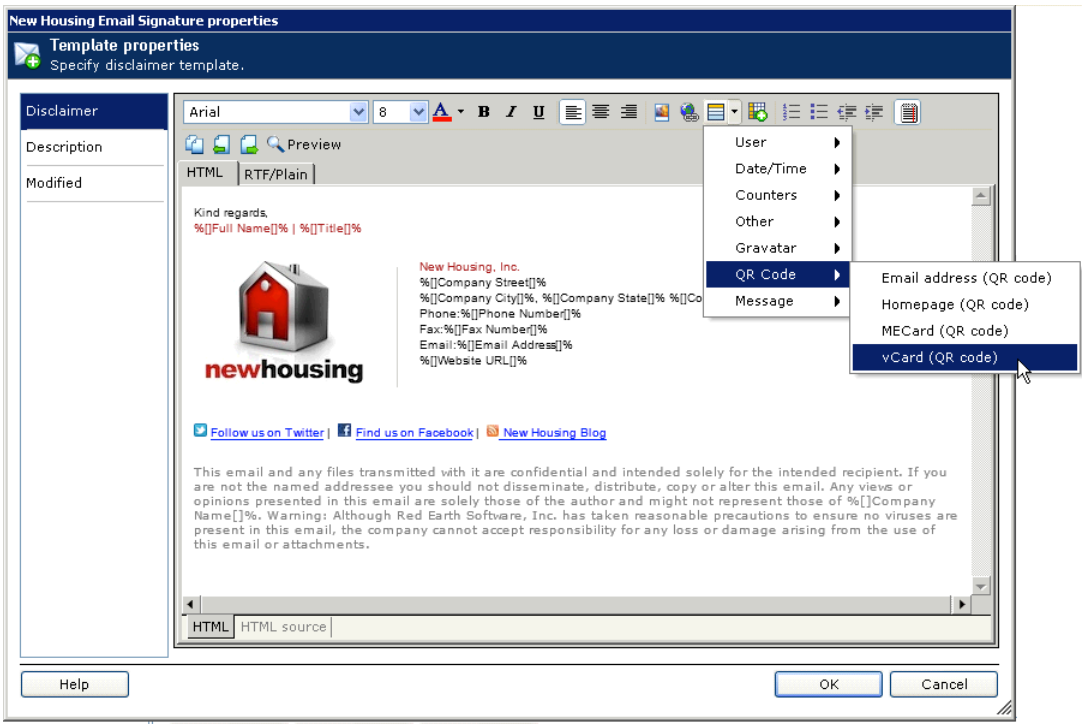
Below is a list of all Gravatar merge fields:

Field Name	Description
About (Gravatar)	Company's name
Display name (Gravatar)	Sender's display name in Gravatar
First name (Gravatar)	Sender's first name in Gravatar
Full name (Gravatar)	Sender's full name in Gravatar
Image (Gravatar)	Sender's image in Gravatar
Image URL (Gravatar)	Sender's image URL in Gravatar
Last name (Gravatar)	Sender's last name in Gravatar
Location (Gravatar)	Sender's Location in Gravatar
Profile link (Gravatar)	Sender's Profile link, e.g. johnsmith (the link points to the Profile URL – see below)
Profile URL (Gravatar)	Sender's Profile URL, e.g. http://gravatar.com/johnsmith



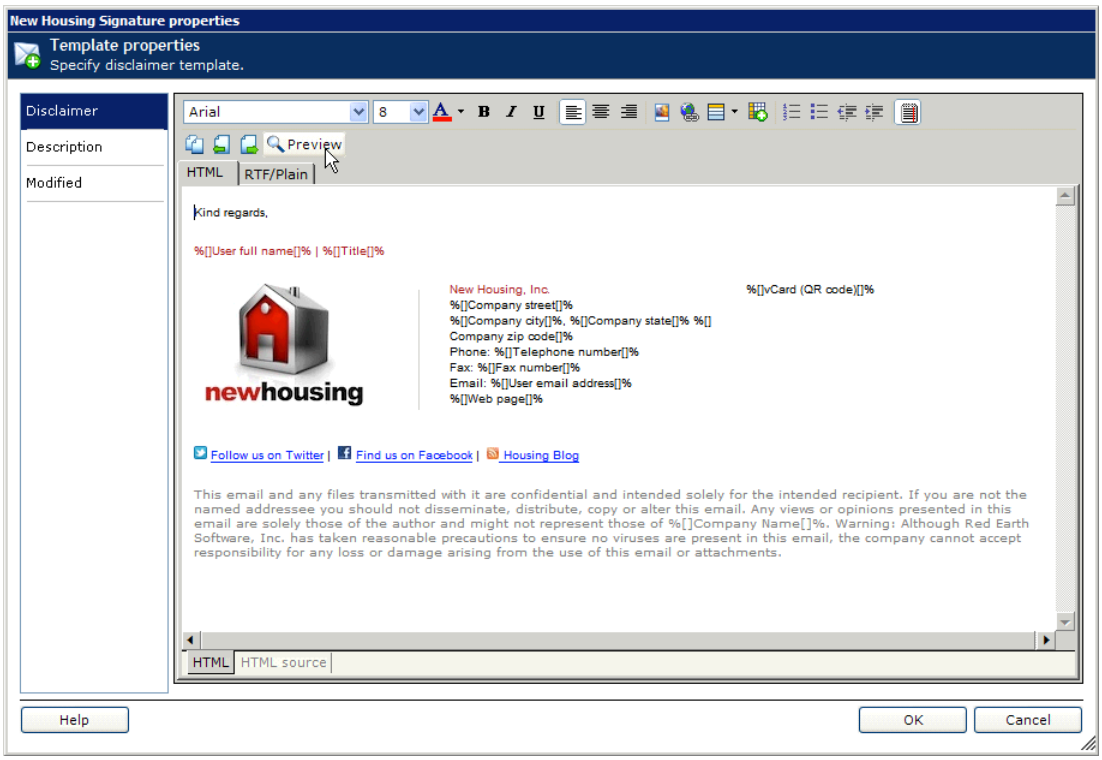
12.5 Inserting a QR Code in the Email Signature

Policy Patrol allows you to insert a QR Code into the email signature with a link to the sender's email address, home page, meCard or vCard. Policy Patrol will automatically generate the QR Code based on the Sender's Active Directory information.

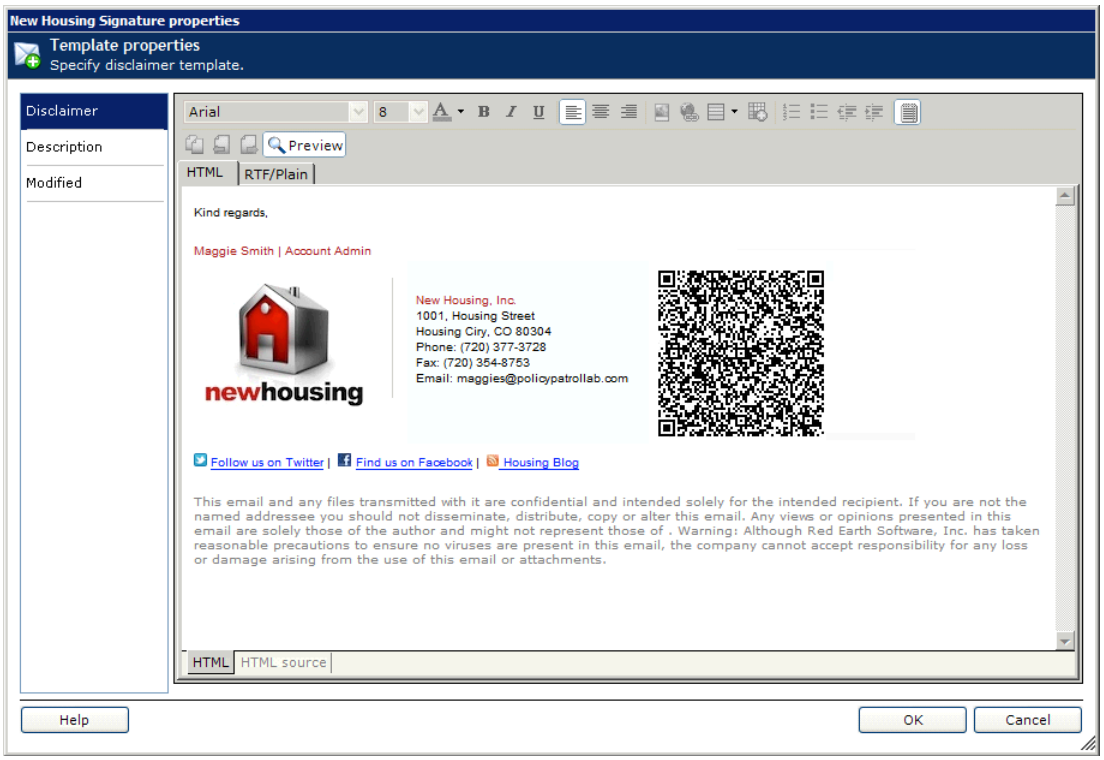


To insert the QR Code merge field into the email signature template, go to **Insert field**, select **QR Code** and the relevant field. Below is a list of the available QR codes:

Field name	Description
Email address (QR code)	Sender's email address as QR Code
Homepage (QR code)	Sender's home page as QR Code
meCard (QR code)	Sender's meCard as QR Code
vCard (QR code)	Sender's vCard as QR Code



Once you have inserted your QR Code merge field, you can click on **Preview** to see the actual QR Code for the selected user.



12.6 Inserting Images or URLs from Active Directory

Policy Patrol allows you to dynamically insert images or URLs from Active Directory, allowing you to insert customize images and URLs for each sender. This can be useful if you are inserting a user's signature or photo, or for instance if you wish to include links to individual bio's.

12.6.1 Inserting an AD Image into the Email Signature

In order to automatically insert an image from Active Directory into your email signature follow the next steps:

1. Enter the image path in an Active Directory custom attribute, for instance: `C:/myimage.jpg`.
2. Add the custom attribute as a merge field in Policy Patrol:
    1. In the Policy Patrol Administration console, go to **Settings** > **Templates**.
    2. Click on **Configure Directory fields** under 'Options'
    3. In **Display Name** enter the Name as you would like it to appear in the list of merge fields, for instance "Image"
    4. Under **Directory Code**, enter the Active Directory Attribute name as listed in ADSI Edit, for instance "extensionAttribute15". Please note that this name is case sensitive. If you are not sure of the name you can check this in ADSI Edit (adsiedit.msc)
    5. Click **OK** to close the dialog.
3. In the Disclaimer/Signature template, insert the link to the image in the HTML source code as follows: `<img src="%[]Image[]%">`.

12.6.2 Inserting a Personalized URL into the Email Signature

Inserting a personalized URL into the email signature can be useful if you would like to include a link to the sender's individual bio or LinkedIn profile. To do this, follow the next steps:

1. Include the user's LinkedIn URL in an Active Directory Custom Attribute, for instance.
2. Add the Custom Attribute merge field in Policy Patrol:
    - In the Policy Patrol Administration console, go to **Settings** > **Templates**.
    - Click on **Directory fields** under 'Options'.
    - In Display name enter the Name as you would like it to appear in the list of merge fields, for instance LinkedIn URL.
    - Under Directory code, enter the Active Directory Attribute name as listed in ADSI Edit, for instance `CustomAttribute9`. Please note that this name is case sensitive. If you are not sure of the name you can check this in ADSI Edit (adsiedit.msc).
3. Insert the custom URL field into the email disclaimer template:
    - In the Policy Patrol Administration console, go to **Settings** > **Templates** > **<folder name>**.
    - Open up your Disclaimer Template.
    - In the HTML tab of the Disclaimer Template, click on HTML Source.
    - In the source, enter one of the options below. Note that in the examples, %[]LinkedInURL[]% is the merge field that contains the user's LinkedInURL.

To create a clickable LinkedIn link:
`<A src="%[]LinkedInURL[]%">LinkedIn</A>` (example: LinkedIn)

To create only a clickable LinkedIn link if the user has a LinkedIn URL in Active Directory:
`%[{LinkedIn}]LinkedInURL[]%` (in HTML this will become: <A href="[LinkedInURL]">LinkedIn</A>) (example for users with LinkedIn URL: LinkedIn, Users with no LinkedIn URL will not get anything added)

To create a clickable LinkedIn image:
`%[{le=<IMG src="http://www.domain.com/images/linkedin.jpg"/>}]LinkedInURL[]%` (in HTML this will become: <A href="[LinkedInURL]"><IMG src="http://www.domain.com/images/linkedin.jpg"/></A>) (example:)

12.7 Editing Templates

To edit an existing template, select the template and click **Edit**. A tabbed dialog will now appear. You will be able to edit the template and change the description. The Modified tab includes information about when the template was last modified and by whom. To rename a template, right-click on the name in the list and select **Rename**. To move a template to a different folder, right-click on the template and select **Move**. Select the folder to move the template to and click **OK**.

Note

If you rename a template that has already been configured for a policy, the policy 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 policy properties and open the dialog where the template is selected. Click **OK** to save the new name in the policy.

12.8 Copying Templates

To copy an existing template, right-click the template and select **Duplicate**. The template will now be duplicated. The name will be displayed as follows: Copy of <original template name>.

12.9 Moving Templates

To move a template to a different folder, right-click on the template and select **Move**. Select the folder you wish to move the policy to and click **OK**. To create a new folder, click the **New...** button.

12.10 Fields

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

Tip

Merge fields can be previewed in the template by clicking on the Preview button in the toolbar (the looking glass icon).

12.10.1 User Fields

The user fields are taken from Active Directory or Lotus Domino, depending on the user import source. 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 **Settings** > **Templates** > **Directory fields**. More information on how to do this can be found in paragraph 13.9 'Configuring additional directory fields'.

Default Field	Description
Company name	Company's name
Fax number	User's fax number
Manager name	Name of user's manager (only for Active Directory)
Manager email	Email address of user's manager
Manager phone	Phone number of user's manager
Manager mobile	Mobile number of user's manager
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
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 **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 paragraph 13.7 'Configuring additional directory fields'.

Upper case/lower case

If you wish certain fields to be displayed in upper case or lower case, you can add a **^** or a **~** character to a field prefix, where ^ converts to UPPER CASE and ~ converts to lower case. For example if you want the user name to appear in upper case, you can enter ^ in the prefix as follows: `%[^]User first name[]%`. This will convert the value of the user name to uppercase, i.e. USER NAME. If you wish to add the user name in lower case, you can enter ~ in the field prefix as follows: `%[~]User first name[]%`. This will convert the value of this field to lower case, i.e. user name.

12.10.2 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.
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).
From: (email)	Email address in the From: field.
From: (name)	Name in the From: field.
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 delivering, deleting or moving the message.
Size of attachment(s)	Size of the attachment(s) in KB. 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(s)	A description of the virus as identified by the anti-virus engine.
X-Sender email	The X-Sender email address, i.e. the email address of the actual sender.
X-Receiver email	The X-Receiver email address, i.e. the email address of the actual recipient(s).
Date sent	Date the message was sent. The date is entered in the default format of the Policy Patrol machine. To change the format, see

	table below.

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.

Note that if you add the **Original message** field to a notification message it is best to enter it in the subject since if you add it to the HTML as well as plain text tab, the message will be attached twice.

12.10.3 Date/Time Fields

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

Field	Description
Time	Current time.
Date	Current date.

To change the date field format, enter the date mask in between the square brackets after the field. For instance, if you enter %[]Current date[MMMM d, yyyy]%, the date will be displayed as February 9, 2012.

Mask	Meaning
d	Day of the month with no leading zero for single digit days
dd	Day of the month with leading zero for single digit days
ddd	Day of the week as three-letter abbreviation, i.e. Mon
dddd	Day of the week as its full name, i.e. Monday
M	Month as digits with no leading zero for single-digit months
MM	Month as digits with leading zero for single-digit months
MMM	Month as three letter abbreviation, i.e. Jan
MMMM	Month as its full name, i.e. January
yy	Year as last two digits, i.e. 12
yyyy	Year represented by full four digits

12.10.4 Other Fields

Other fields include counters that can be used to add an ID number that is automatically increased. For instance, if you include the 'Unique counter 1' field in the subject of a notification message, the counter ID will be increased with a value of 1 each time the notification message is sent. This can be useful for applying tracking numbers to mails received on or sent to certain addresses. Notification messages can also include tracking numbers.

Field	Description
Annually reset counter	Counter will reset annually.
Daily reset counter	Counter will reset daily.

Monthly reset counter	Counter will reset monthly.
Unique counter	Counter will never reset.
Challenge/response link	Link to the IIS website for challenge/response.
Policy name	Name of the policy that triggered

Policy Patrol includes two counters of each to enable you to create multiple counters of the same type. If you require more counters, please contact Red Earth Software technical support.

The suffix of the counters can be used to customize the way in which the counter is displayed. For instance, it is possible to specify the number of digits of the counter by entering a zero for each number in the suffix of the field, as follows: `%[]Unique counter 1[0000]%`. If four zeros are added the counter value will always be 4 digits (i.e. 0001, 0002, etc.). If eight zeros are added in the suffix, for instance `%[]Annually reset counter[00000000]%`, the counter value will always be 8 digits (i.e. 00001234, 00001235, etc.).

You can also use the counter fields in conjunction with date fields, for example: `INV-%[]Date[yyyyMM]%-%[]Monthly reset counter[0000]%`. This would result in INV-201307-0001, INV-201307-0002 etc. When the month changes, the Monthly reset counter field will reset and it would start with INV-201308-0001, INV-201308-0002, etc.

12.11 Inserting AD Fields Depending on User's AD Information

Sometimes not all users have the same Active Directory fields. For instance, perhaps not all users have a cell phone entry in Active Directory. Policy Patrol allows you to get round these differences while still allowing you to configure only one template:

12.11.1.1 Using a Prefix only if the Field Exists

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 properties.

12.11.1.2 Avoiding an Empty Line if a Field Does Not Exist

To **avoid an empty line** when a field does not exist you must enter \n in the field prefix %[]% (this stands for a line break and since it is entered in the prefix it will only be applied if there is a field value). For instance if you want the user name to appear, followed by the title field (if it exists), you can enter the following in the Disclaimer template: %[]User full name[]%%[\n]Title[]%. If you want to combine it with a field prefix, you must enter this as follows: %[]User full name[]%%[\nTitle:]Title[]%...

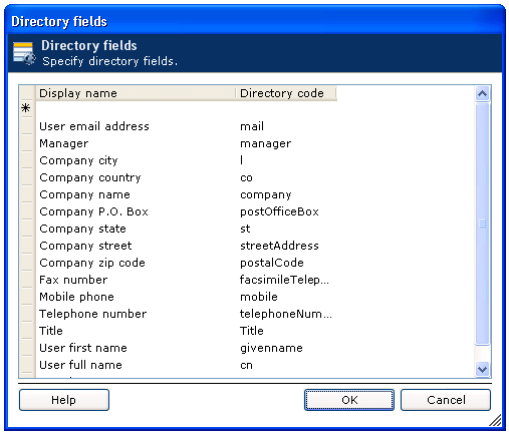
12.11.1.3 Specifying a Default Value if a Field Does not Exist

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.

12.12 Configuring Additional Directory Fields

Directory fields can be configured from **Settings** > **Templates** > **Directory fields**. Policy Patrol already includes a number of merge fields taken from Active Directory. You can add more fields by entering the **Display name** (this is the name that will be displayed in Policy Patrol) and the **Directory code** (this is the actual code for the field in the directory). Click **OK**.



For more information on how to find the correct directory codes for Active Directory, consult the following document:

How to enter additional AD fields in Policy Patrol
(http://www.policypatrol.com/assets/pp10-adfields.pdf)

The table below lists several codes that can be used for Lotus Domino.

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

Tip

Remember that each Directory type uses a different field code. For instance, Active Directory uses the 'url' code to identify the company's home page. However, this might not be the same for Lotus Domino. Therefore, if you have imported users from different import sources 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.

Chapter 13

Quarantined Messages

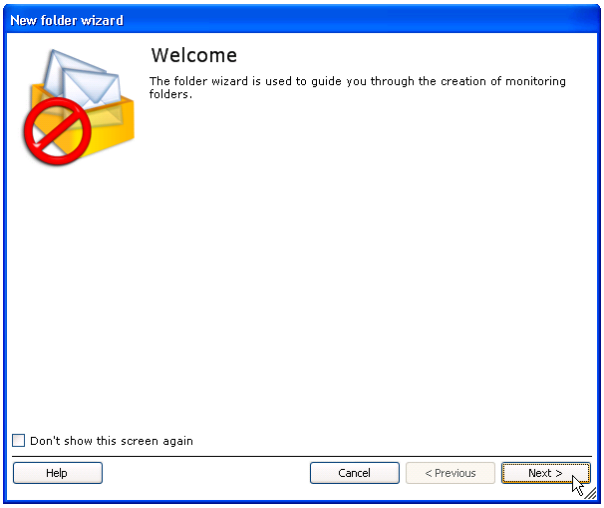
This chapter discusses how to configure quarantine folders and how to view messages in the quarantine folders via the Policy Patrol Administration console and Web manager. It also discusses how you can set security permissions for each quarantine folder.

13.1 Creating Quarantine Folders

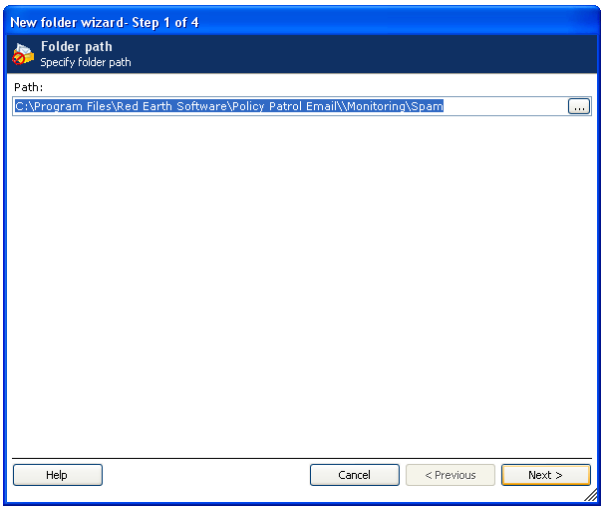
Policy Patrol includes a number of sample quarantine folders. To create your own quarantine folder:

1. Right-click **Quarantine folders** and select **New Folder...**.

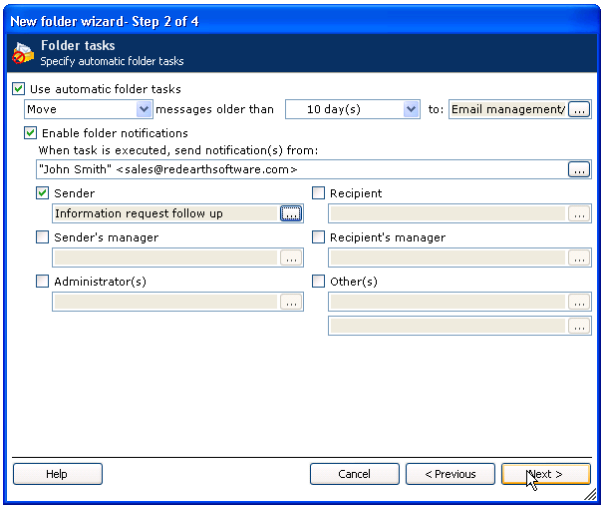
2. The monitoring folder wizard will appear. In the Welcome screen, click **Next**.



3. Enter or browse to (only available on the local machine) the folder location where the messages should be stored, for instance C:\Program Files\Red Earth Software\Policy Patrol Email\\Monitoring\Spam. Note that monitoring folders should always be located in the Red Earth Software\Policy Patrol Email\Monitoring directory. Click **Next**. If the folder does not yet exist a message will be shown asking whether you wish Policy Patrol to create the folder. Click **Yes**.



4. If you wish Policy Patrol to perform automatic folder tasks, tick the box **Use automatic folder tasks**. You can select to **Move**, **Delete** (this will permanently delete the message) or **Deliver** emails older than x number of minutes, hours, days, weeks or months. If you select to move messages, you must select the folder to move the messages to.



Tip

To avoid deleting legitimate emails by mistake, you can configure a Deleted monitoring folder and place spam messages older than for instance 2 days in this folder. Messages in the Deleted folder older than 30 days can be permanently deleted. In case a user wishes to release a legitimate message out of quarantine, this would still be possible for 30 days after receipt of the message.

When the automatic task is performed, i.e. the message is moved, deleted or delivered, you can configure a notification to be sent. For instance you can send an automated follow up after a specified time frame. To configure a notification, select the option **When task is**

executed, send notification(s) from:. Enter the From: field to be used in the email message, select the recipient and select the Notification template to be used by clicking on the **...** button. When you are ready, click **Next**.

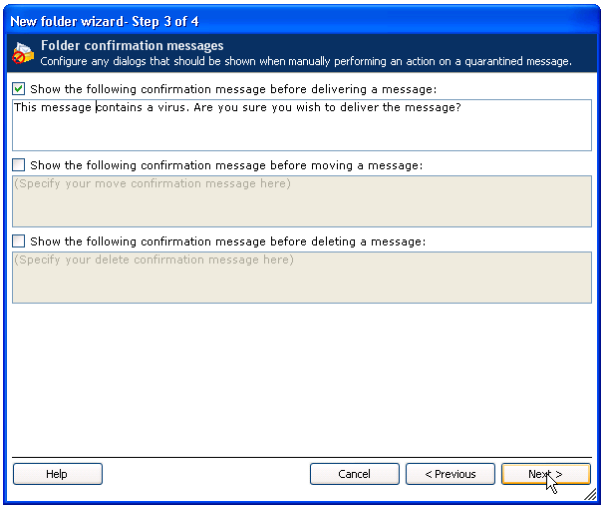
Tip

Since the moving of messages can be combined with a notification message, this feature can be useful for automated lead follow up. For instance you could configure Policy Patrol to send a follow up message x number of days after an information request was received. For more information on how to configure this, consult the following document: How to configure email management with Policy Patrol, (http://www.policypatrol.com/assets/pp10-emailmanagement.pdf)

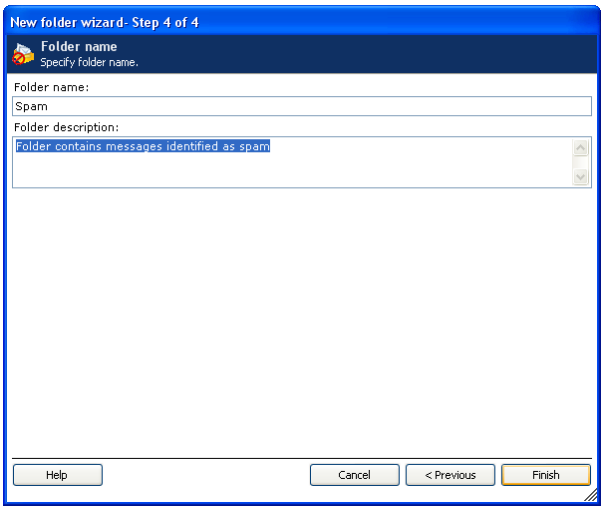
Note

Remember that Policy Patrol will perform automatic folder tasks approximately once every 30 minutes. This means that it can take up to 30 minutes for items to be deleted or moved after you configure automatic folder tasks.

5. Configure any pop-up dialogs that should be shown when manually performing an action on a quarantined message; such as deleting, moving or delivering the message. For instance you could configure a warning message to be shown when messages in the virus folder are delivered. Click **Next**.

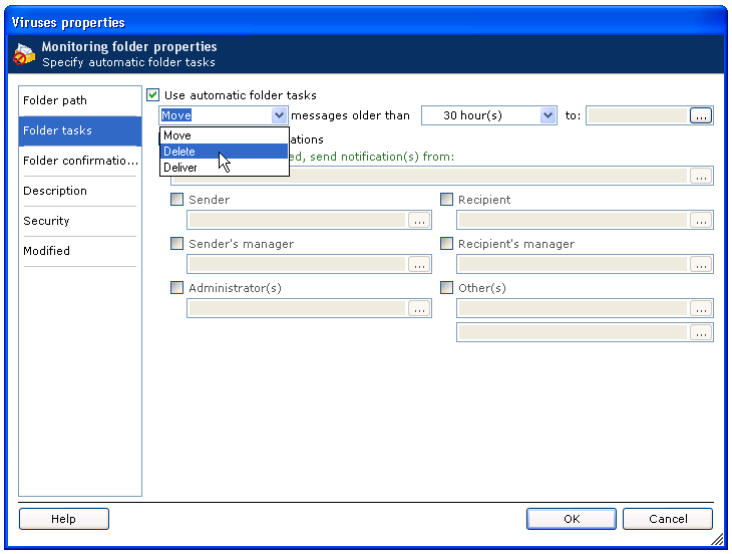


6. Enter a name and description for the monitoring folder and click **Finish**.



13.2 Editing Quarantine Folders

To edit the properties of a quarantine folder, right-click the folder and select **Folder properties**. A tabbed dialog will now appear. Make the necessary changes and click **OK**. To delete a quarantine folder, right-click and choose **Delete folder**.



Note

If you are going to use challenge/response, you must not remove or rename the Challenge/Response folder.

13.3 Quarantine Folder Permissions

Each folder can be assigned different rights for different users. These rights determine which users can access the quarantined messages in the monitoring folder. The messages can be accessed in three ways:

- Policy Patrol Administration console (provides access to all messages in the folder): By default all members of the Administrative Group in Active Directory can access the Administration console, unless users are selected under **<server name>** > **Security** > **User security**. In this case only the users that are listed have access to the Administration console. The users listed under **<server name>** > **Security** > **User security** can be further distinguished into two classifications: users without Administrator privileges and users with Administrator privileges. The first group can be denied access to certain parts of the Administration console and the second group cannot. For more information on this consult the paragraph 20.1.1 'User access rights'.

- Web Manager - Administrator version (provides access to all messages in the folder): Only Policy Patrol Administrators (by default these are all members of the Administrative Group in Active Directory, or if users are selected under **<server name>** > **Security** > **User security**, only the users that are listed and have been assigned Administrator rights) can access the Administrator version of the Web manager.

- Web Manager - User version (provides access to only the user's messages in the folder): All users can access the User version of the Web manager, however they can only access the folders for which they have been given permissions.

Tip

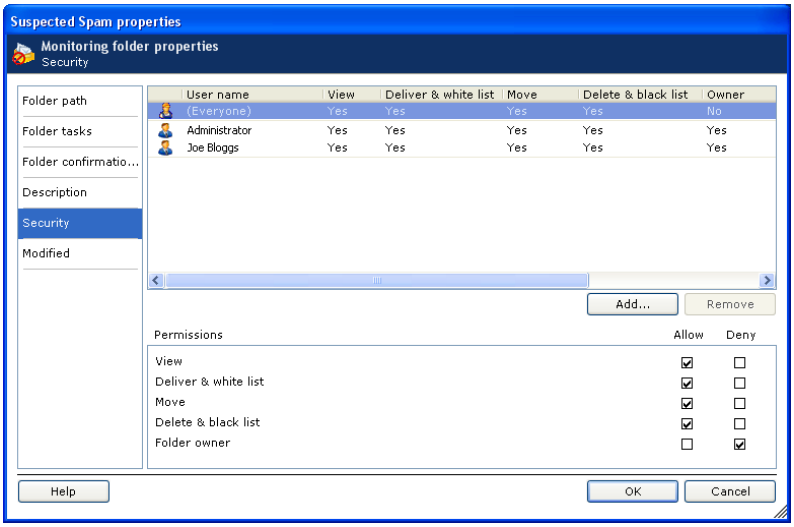
By default, new monitoring folders are created with full rights for Everyone. This means that if you want all your users to be able to access only their own messages (and delete, move and deliver items) in every monitoring folder and you want to allow members of the Administrative group to access all messages, you do not need to configure anything since Policy Patrol rights are already configured in this way by default.

By default the (Everyone) group has full access to the folder. To change these permissions:

1. Go to **Quarantine**, right-click the folder and choose **Folder Properties**.

2. Go to the **Security** tab. By default the (Everyone) group has full access to the folder. To change permissions, select the group and change the Allow/Deny permissions. The following rights can be applied:

Right	Description
View	View items
Deliver & add to allow list	Deliver items and add to allow list
Move	Move items
Delete & add to block list	Delete items and add to block list
Folder owner	Change folder permissions



If you only wish certain users to have rights to the folder, click on **Add** and select the user(s) with the permissions. Select **Allow** or **Deny** for the relevant rights. Then select **Everyone** and click **Deny** for all rights.

If you wish all users to have access to the folder apart from a couple of exceptions, click on **Add** and select the users to be denied access. Select the user(s) and tick the **Deny** check boxes.

A Folder owner has the right to change the folder permissions for the folder. Therefore, if you wish to deny permissions for a user, you must also select **Deny** for the **Folder owner** right.

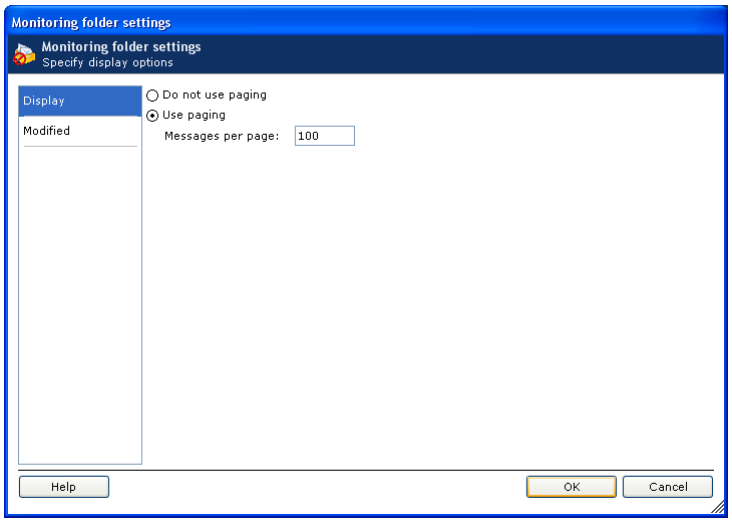
Remember that each folder needs to have at least one Folder owner and that Administrators cannot be denied any permissions.

Note

Policy Patrol Administrators have full rights to all components and folders and cannot be denied any permissions. If you wish to block access for a user with Administrator rights, you must first remove the Administrator rights for the user in **<server name>** > **Security** > **User security**.

13.4 Quarantine Folder Settings

The quarantine folder settings are found in **Quarantine** > **Configure quarantine folders...**. These settings allow you to configure the display options for the folder. If you want to display all messages on one page, select the option **Do not use paging**. If you wish to view a limited number of messages on one page to increase display times, select the option **Use paging** and enter the number of messages to display per page.



Note

These options only apply to the monitoring folders in the Administration console. If you wish to change the messages per page in the web manager, you can do so by opening Web.config located in Program Files\Red Earth Software\Policy Patrol Email\Web\Manager and changing the number in the following key: <add key="PageSize" value="25"></add>. For instance if you want to view 50 messages per page you must change 25 to 50: <add key="PageSize" value="50"></add>.

13.5 Viewing Messages via the Administration Console

To view messages on hold in the Policy Patrol Administration console, go to **Quarantine** and select the appropriate folder. You will now see a list of all items on hold.

For each message the Date processed, Sender, Recipients, Subject, Size and Additional information will be displayed. The list can be ordered by clicking on the column headers (only if you have paging disabled in **Quarantine** > **Configure quarantine folders...**. To view more details of the message, select the message in the top pane and click on the items in the bottom pane.

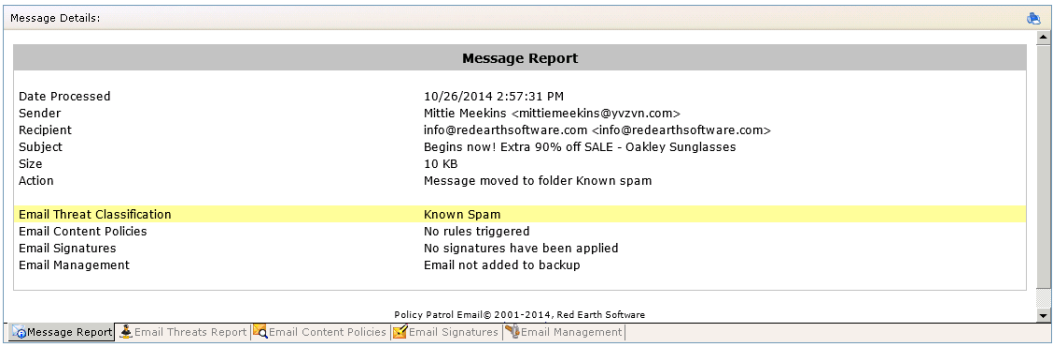
Messages that have not yet been opened in the Administration console are marked with an 'unread' icon ( ) and messages that have been opened are marked with a 'read' icon ( ).

For each message, the following information will be shown:

13.5.1 Message Report

To view the details of the message, select the message in the top pane. The bottom rigeht pane will display the message report. The Date processed, Sender, Recipients, Subject, Size and Action will be shown for the message and it will display whether the message was considered as

spam, contained a virus, archived or whether it triggered a policy. The reason for quarantining the message will appear highlighted.

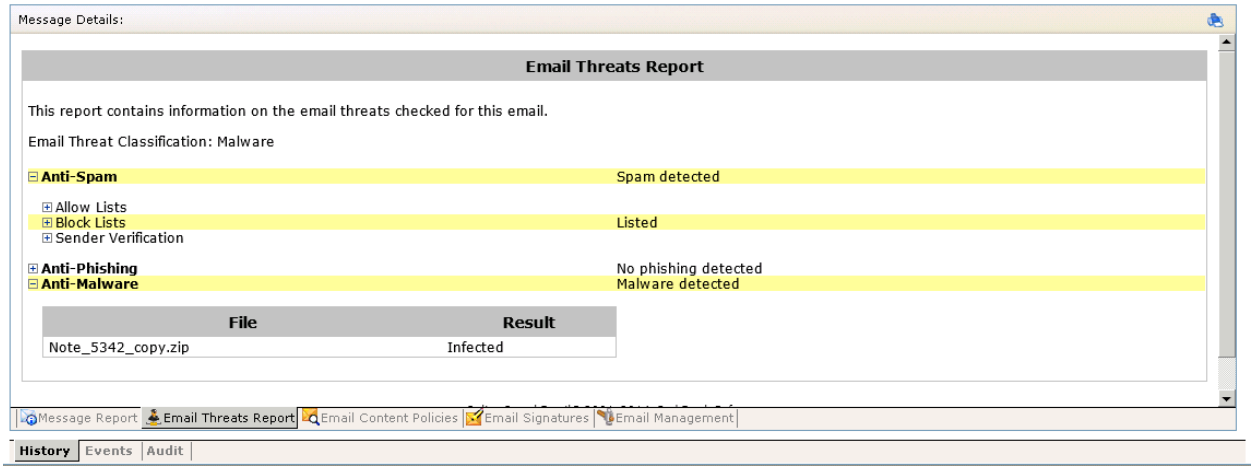


13.5.2 Viewing Message Text and Headers

To view the message text for external messages, in the left column expand **multipart/alternative** and select **text/plain** or **text/html**. If you select **text/plain**, you will see the plain text version of the message in the right pane. To view the headers of the message, click on the **Headers** tab. If you select **text/html**, you will see the HTML version of the message in the right pane. By default it first displays the **HTML Source** in order to avoid downloading any pictures. If you wish to view the message including pictures, you can select the **HTML** tab. A message will be shown warning that scripts and pictures will be loaded. Click **Yes** to proceed. To view the headers of the message, select the **Headers** tab.

13.5.3 Email Threats Report

This report includes information on the message origin and the results of each individual anti-spam check that was performed. The reason why the message was quarantined will appear highlighted in the report. For instance in the screen below, the message was blocked because it reached the threshold of words on the block list. If words are found in the message, they will be displayed together with the score and threshold. To print the report, click on the **Print** icon in the top right hand corner.



13.5.4 Email Content Policies Report

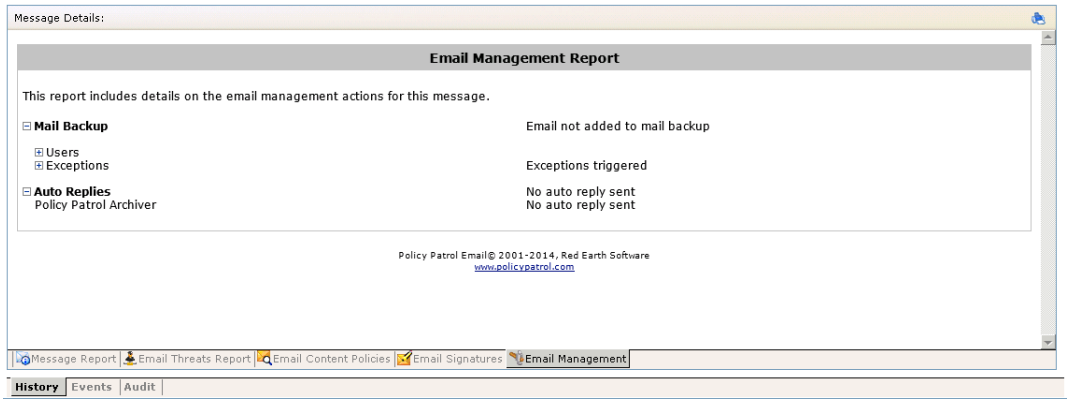
This report includes a list of all policies that were processed and whether they triggered for the message. The policies that triggered will be highlighted. To print the report, click on the **Print** icon in the top right hand corner.

13.5.5 Email Signatures Report

This report displays whether the message was scanned for viruses and if a virus was found. If a virus was found, the name will be listed. To print the report, click on the **Print** icon in the top right hand corner.

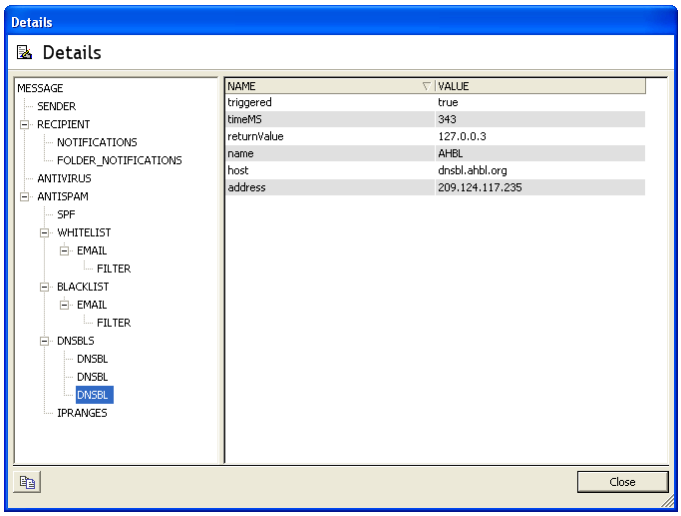
13.5.6 Email Management Report

This report displays whether the message was archived. To print the report, click on the **Print** icon in the top right hand corner.



13.5.7 Viewing Details

To view further details for the message, right-click the message and choose **Details**. The details dialog will include information on the results of each spam filtering method and policy that was processed and if relevant will list any words found and their score. To copy the complete details to a text file, click on the **Copy** button in the bottom left hand corner and paste into a text file.

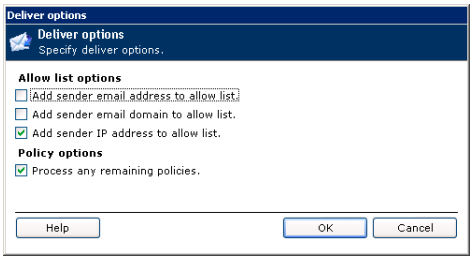


13.5.8 Saving Down Attachments

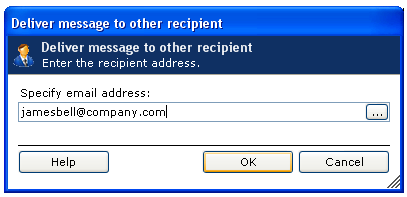
If you wish to view or save down an attachment, click on the attachment. A dialog will appear asking you to open or save the file.

13.5.9 Delivering Messages On Hold

To deliver a quarantined or delayed message, select the message and click on the **Deliver** button. The deliver options dialog will appear. You can select to add the sender email address to the allow list or add the sender IP address to the allow list. You can also select to process any remaining policies on the message before delivering it.



If you wish to deliver the message to a different recipient, you can right-click the message and select the option **Deliver to other**. Enter the email address to deliver the message to and click **OK**. Now the Deliver options dialog will be displayed as described above.

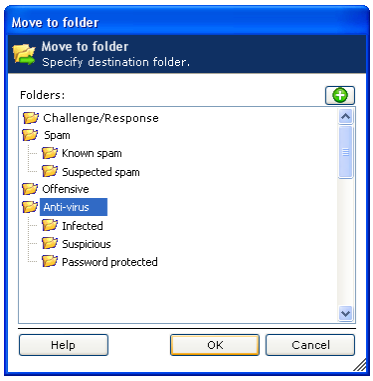


13.5.10 Deleting Messages on Hold

To delete a quarantined or delayed message, select the message and click on **Delete**. The message will be permanently deleted.

13.5.11 Moving Messages on Hold

If you wish to move a message to another folder, select the message and click **Move**. A dialog will pop up with available monitoring folders. Select the folder to move the message to and click **OK**.



13.5.12 Multiple Messages

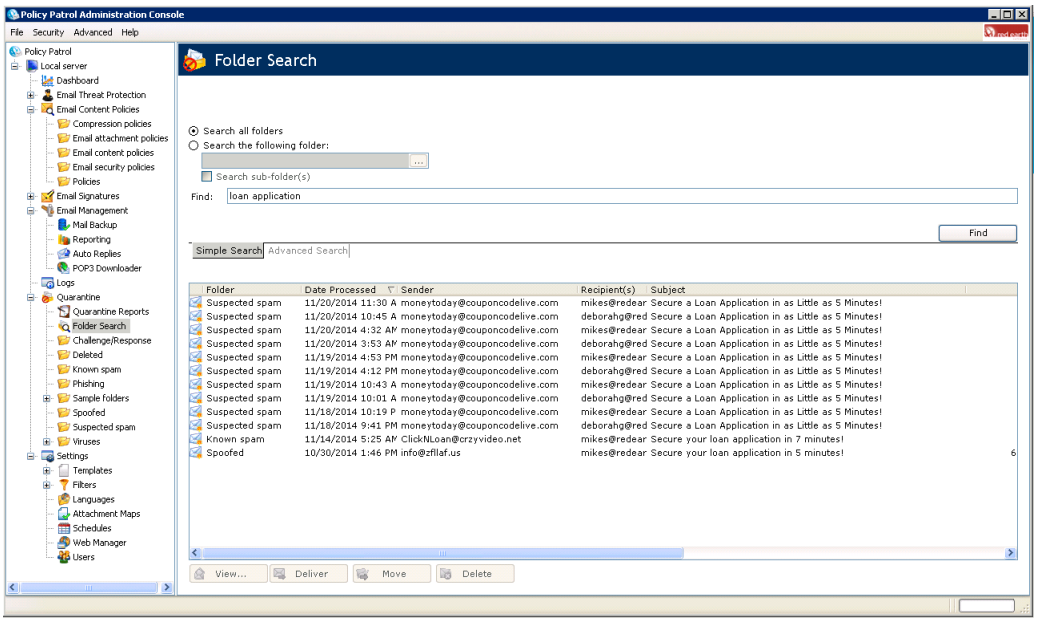
You can deliver, delete or move multiple messages, by selecting the appropriate messages and clicking on the **Deliver**, **Delete** or **Move** button. To select multiple messages in a row you can use the [SHIFT] and the arrow keys. To select separated messages hold [CTRL] pressed and click on each message that you wish to select. Finally, to select all messages press [CTRL+A].

13.5.13 Folder Search

Go to **Quarantine** > **Folder Search** (or click on the **Search** link at the top of a monitoring folder) to search for certain messages. The simple search allows you to search for a word or email address in the message. Advanced search allows you to specify more precisely in which field the word or email address should be present.

13.5.13.1 Simple Search

To perform a simple search, click on the **Simple Search** tab. Specify whether you wish to search all folders or whether you wish to search only selected folders. If you wish to include subfolders in your search, check the option **Search sub-folder(s)**. Enter the word(s) or email address that you are searching for and click **Find**. Policy Patrol will search all fields (attachment names, policies triggered, date sent, date processed, X-sender, X-receiver, From:, To:, Cc: and subject) and will display the search results in the bottom pane. You can also enter a domain name, for instance `company.com`. It is not possible to use wildcards in your search but you can enter part of a word. For example, if you enter the word `house`, Policy Patrol will find emails with 'house' or 'houses' in the subject and emails from the domain 'house.com' and 'openhouses.com'.



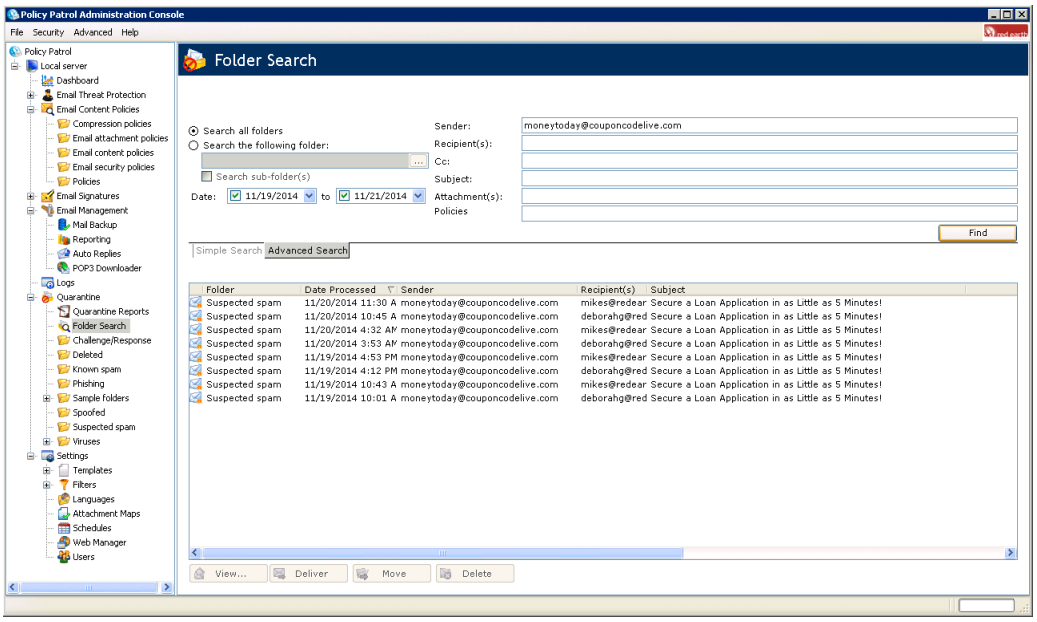
13.5.13.2 Advanced Search

To perform an advanced search click on the **Advanced Search** tab. Specify whether you wish to search all folders or whether you wish to search only selected folders. If you wish to include subfolders in your search, check the option **Search sub-folder(s)**. You will be able to search the following fields:

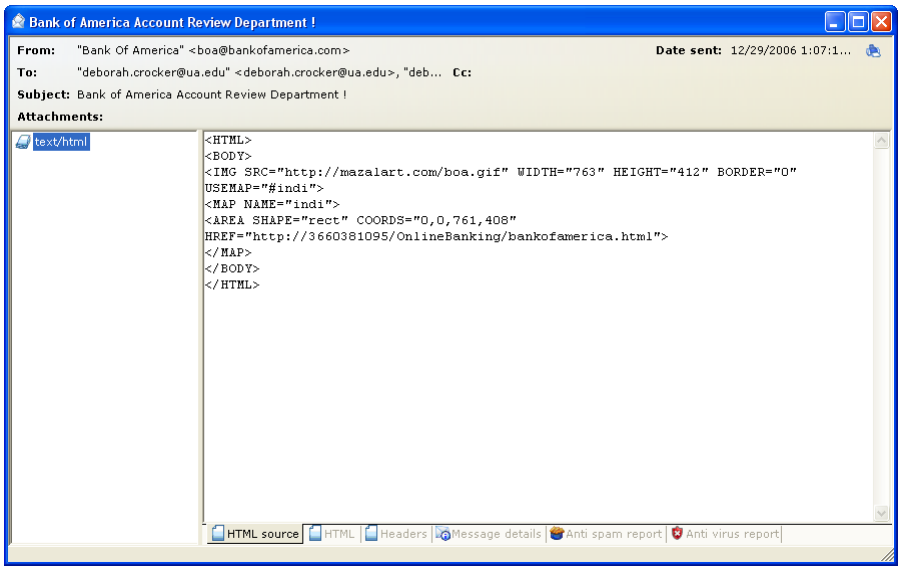
Search Field	Searches in:
Sender	From: and X-Sender fields
Recipient(s)	To: and X-Receiver fields (includes Bcc and Cc recipients)
Cc	Cc: field
Subject	Subject of the message
Attachment	Attachment name
Policy triggered	Name of the policy that triggered for the message
Date	Date the message was sent

In the Sender and Recipient fields you can enter a complete email address or a domain name. For instance if you enter `company.com`, Policy Patrol will find messages to or from 'sales@company.com' and 'info@newsletters.company.com'. In the Policy triggered field, enter the name of the policy (or part of the name) that triggered for the message. For instance if you enter the word `offensive`, Policy Patrol will find the messages that triggered the policy 'Quarantine offensive content'. It is not possible to use wildcards in your search but you can enter part of a word. For example, if you enter the word `house`, Policy Patrol will find emails with 'house' or 'houses' in the subject or attachment name and emails from the domain 'house.com' and 'openhouses.com' (depending on the field where you entered your query).

When you are ready entering your search criteria, click **Find**.



To view a selected message, click on **View**. The same reports will be available as specified in paragraphs 13.5.1 to 13.5.12.



13.5.14 Quarantine Reports

Quarantine reports allow you to email reports containing newly quarantined items to users and Administrators. Messages can be viewed, deleted and delivered from the quarantine report. There are two types of quarantine reports;

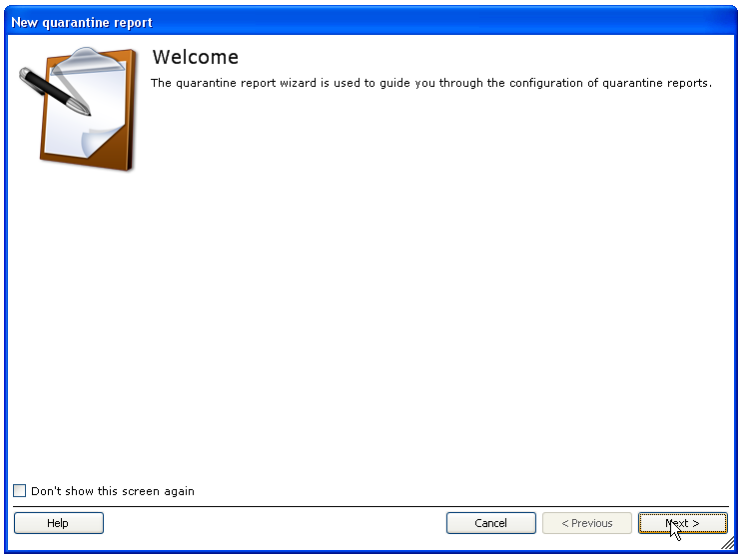
1. **User reports** - Reports only include the emails for the user that the report is emailed to.

2. **Administrator reports** – Reports include messages for all or selected users.

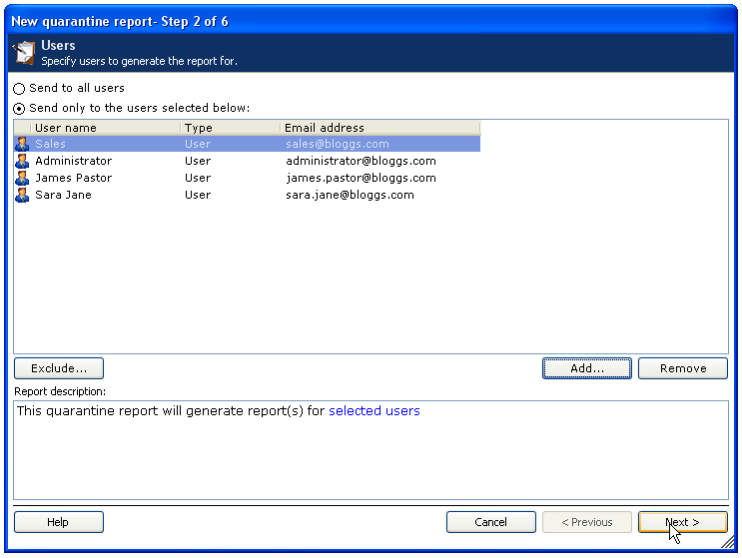
13.5.14.1 Configuring a User Quarantine Report

To configure a user quarantine report (includes only the user's emails), follow the next steps:

1. Go to **Quarantine** > **Quarantine Reports**. Click **New**.
2. The quarantine report wizard will start up. In the Welcome dialog, click **Next**.

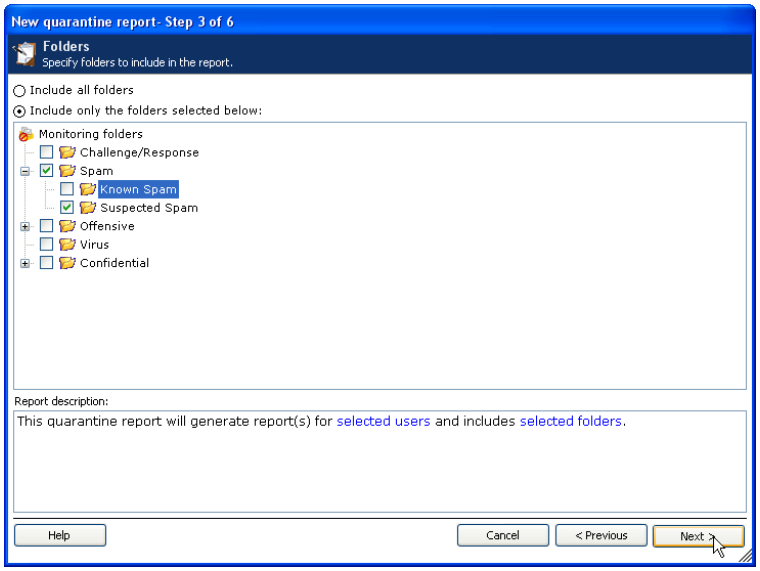


3. Select **User Report** and click **Next**.
4. To email the report to all users, select the option **Send to all users**. If you only wish to send the quarantine report to selected users, enable the option **Send only to the users selected below**. Click on **Add** to select the users. When you are ready, click **Next**.

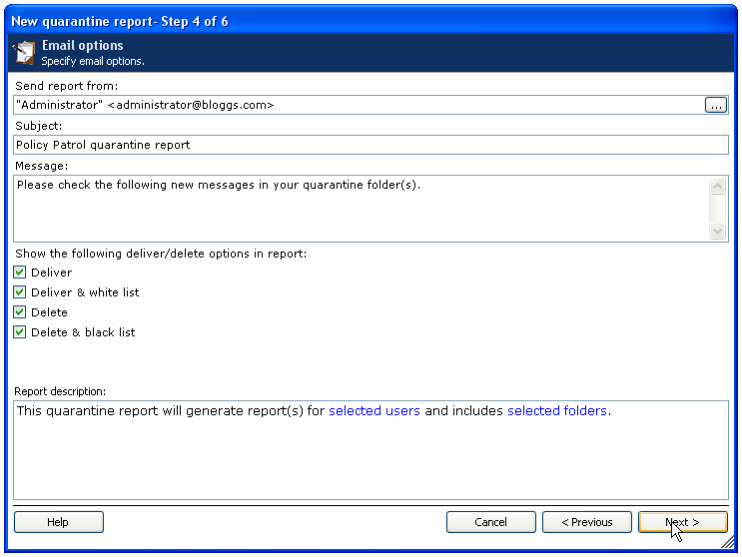


5. Select which folders you wish to include in the quarantine report. To include messages from all folders in the report, select **Include all folders**. To include only messages from

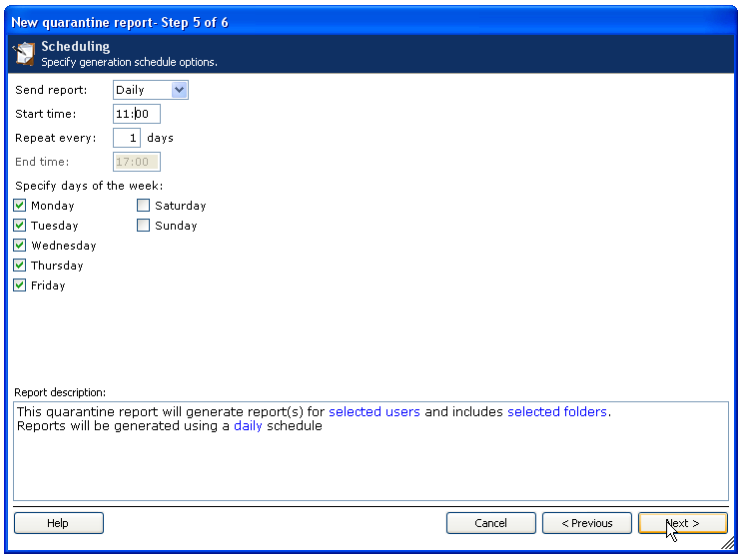
certain folders, select **Include only the folders selected below** and select the folders to be included. Click **Next**.



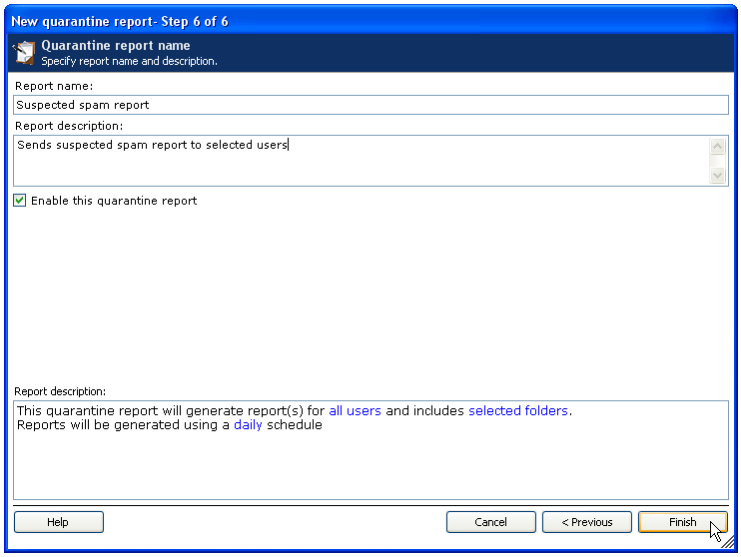
6. Configure the options for the email message. You can specify the From: email address, the subject and a message. You can also select whether the user sees the options **Deliver**, **Deliver & add to allow list**, **Delete** and/or **Delete & add to block list** in the quarantine report. When you are ready click **Next**.



7. Now you must specify when and how often the report is emailed. You can configure the report to be sent daily, hourly or weekly and how often to send the report. For instance if you want the report to be sent once every two hours, select **Hourly** and enter 2 in 'Send every'. If you select hourly you will be able to specify an end time. Select the days of the week that you want the report to be sent. When you are ready, click **Next**.



8. Enter the name and a description for the report. If you wish the report to be enabled, select the option **Enable this quarantine report**. Click **Finish** to create the report.

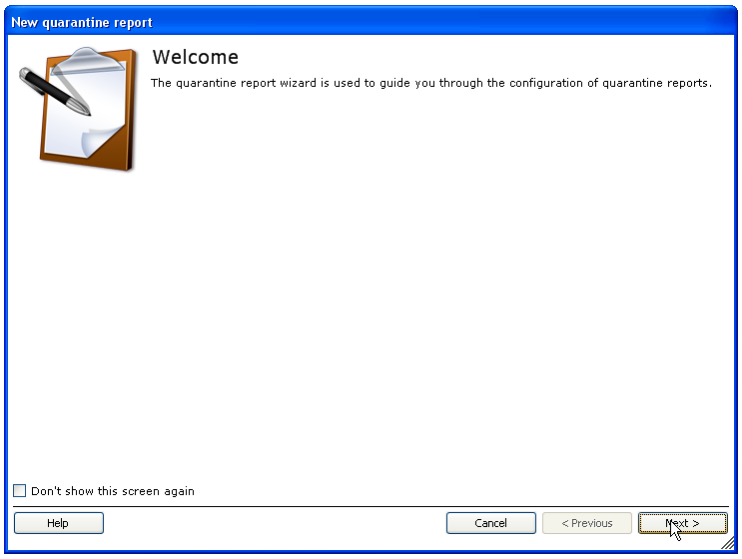


13.5.14.2 Configuring an Administrator Quarantine Report

To configure an Administrator quarantine report (includes specified users' emails), follow the next steps:

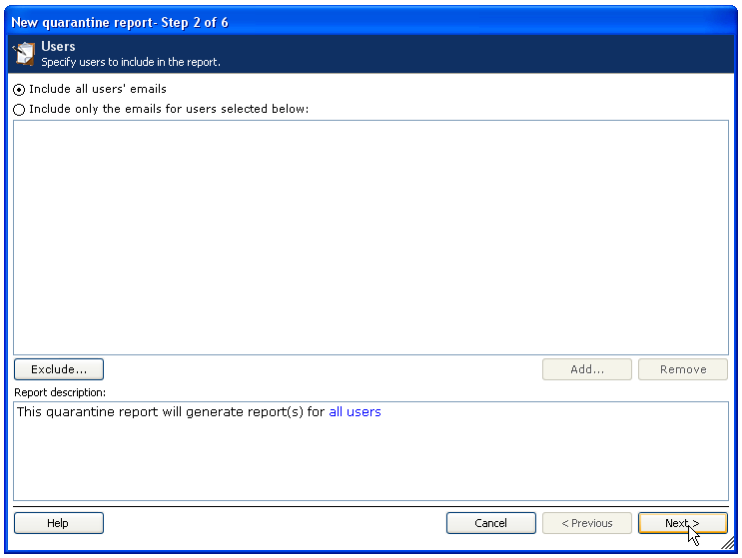
1. Go to **Quarantine** > **Quarantine Reports**. Click **New**.

2. The quarantine report wizard will start up. In the Welcome dialog, click **Next**.

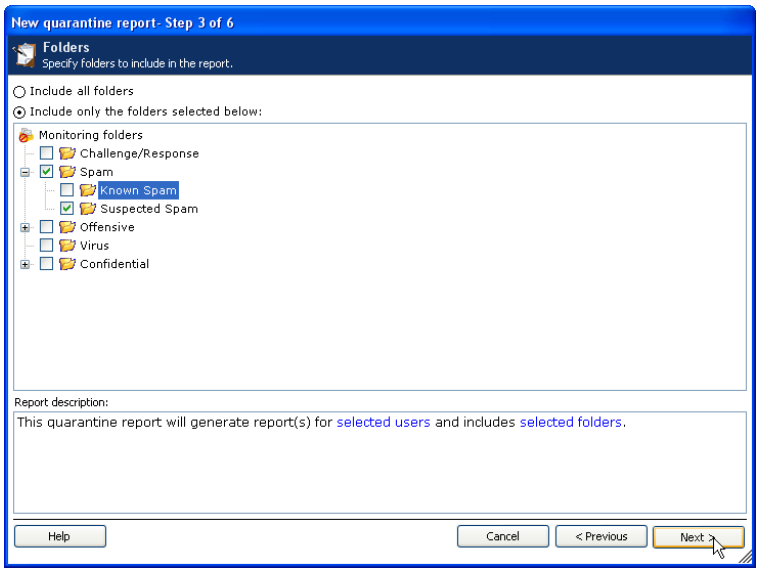


3. Select **Administrator Report** and click **Next**.

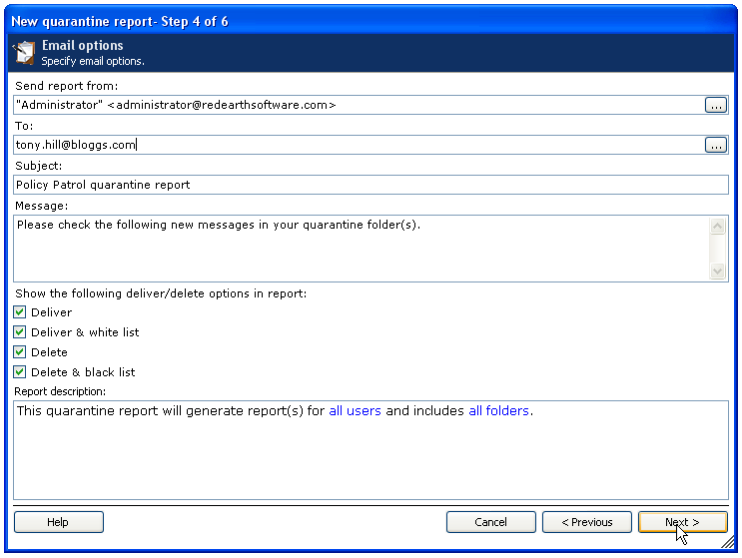
4. To include all users' emails in the report, select the option **Include all users' emails**. If you wish to exclude certain users from the report, click on the **Exclude...** button. If you only wish to include selected users' emails in the report, enable the option **Include only the emails for users selected below**. Click on **Add** to select the users. When you are ready, click **Next**.



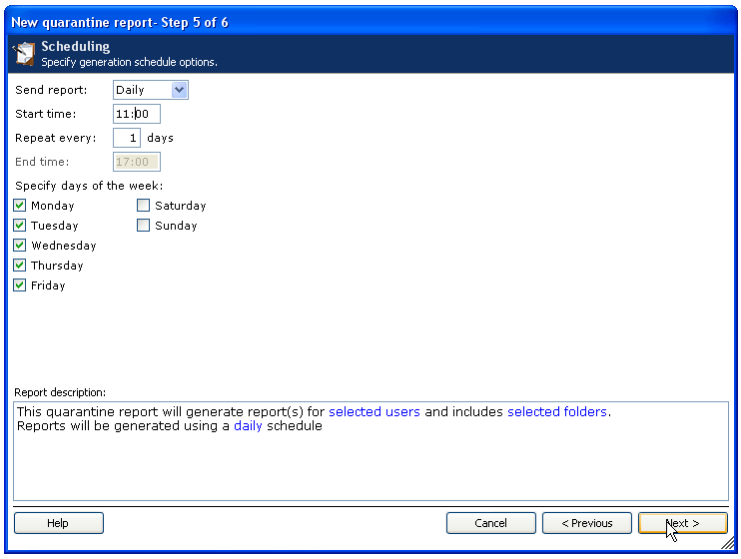
5. Select which folders you wish to include in the quarantine report. To include messages from all folders in the report, select **Include all folders**. To include only messages from certain folders, select **Include only the folders selected below** and select the folders to be included. Click **Next**.



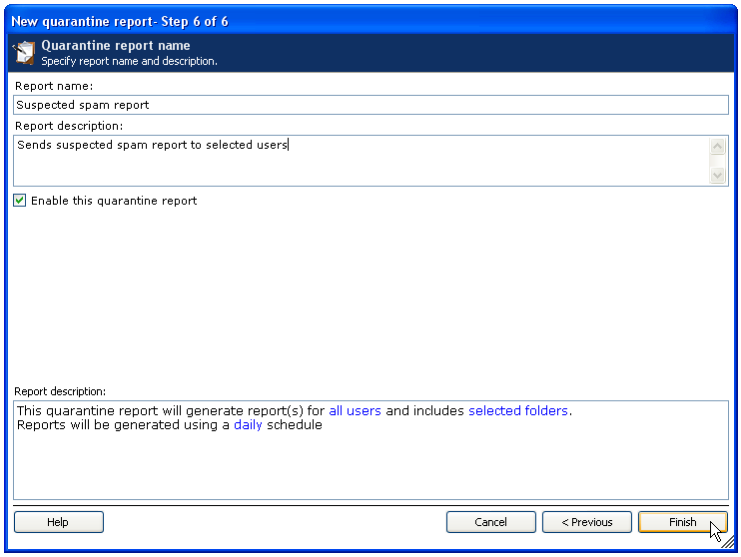
6. Configure the options for the email message. You can specify the From: email address, To: email address, the subject and a message. You can also select whether you want to see the options **Deliver**, **Deliver & add to allow list**, **Delete** and/or **Delete & add to block list** in the quarantine report. When you are ready click **Next**.



7. Now you must specify when and how often the report is emailed. You can configure the report to be sent daily, hourly or weekly and how often to send the report. For instance if you want the report to be sent once every two hours, select **Hourly** and enter 2 in 'Send every'. If you select hourly you will be able to specify an end time. Select the days of the week that you want the report to be sent. When you are ready, click **Next**.

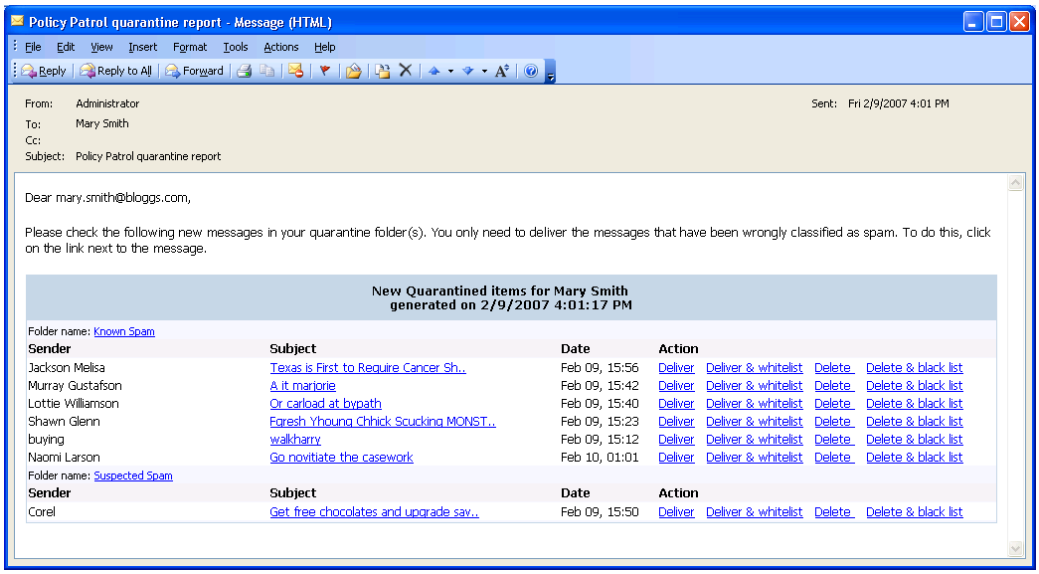


8. Enter the name and a description for the report. If you wish the report to be enabled, select the option **Enable this quarantine report**. Click **Finish** to create the report.



13.5.14.3 Viewing the User Quarantine Report

The user quarantine report contains a list of all newly quarantined items for the user in the selected folder(s). A quarantine report is only sent when there are newly quarantined messages. The user quarantine report lists the Sender, Subject and Date for each newly quarantined item. To view the details of the message, the user can click on the subject line. Next to each message the different options will be listed: Deliver, Deliver & add to allow list, Delete and/or Delete & add to block list (the options displayed depend on the selection in the Quarantine report configuration). The folder name will also be displayed as a link. If the user clicks on this link, the Policy Patrol Web Manager will pop up and (after verifying user credentials) will display all their messages in the monitoring folder (only their own messages).



Note

To allow the user to view and deliver messages you must give the user at least view and deliver & add to allow list rights to the monitoring folder (see paragraph 13.3 Quarantine folder permissions). By default everyone is given access to the Known spam and Suspected spam folders.

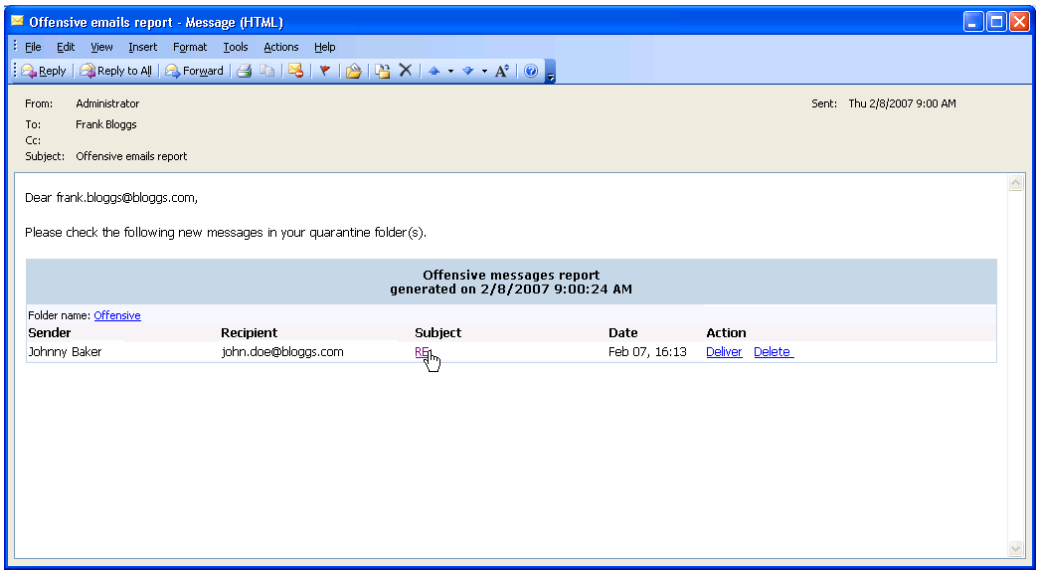
The documents below will help you inform your users about how to use the Policy Patrol quarantine reports and Web Manager. Both documents are in Microsoft Word so that you can place your own logos and enter the correct Web Manager links before distributing the documents amongst your users:

Policy Patrol User Memo
(http://www.policypatrol.com/assets/pp10-usermemo.doc)

Policy Patrol User guide
(http://www.policypatrol.com/assets/pp9-userguide.doc)

13.5.14.4 Viewing the Administrator Quarantine Report

The Administrator quarantine report contains a list of all newly quarantined items in the selected folder(s). A quarantine report is only sent when there are newly quarantined messages. The Administrator quarantine report lists the Sender, Recipient, Subject and Date for each newly quarantined item. To view the details of the message, click on the subject line. Next to each message the different options will be listed: Deliver, Deliver & add to allow list, Delete and/or Delete & add to block list (the options displayed depend on the selection in the Quarantine report configuration). The folder name will also be displayed as a link. If you click on this link, the Policy Patrol Web Manager will pop up and (after verifying Administrator credentials) will display all the messages in the folder (any sender or recipient).



13.6 Viewing Quarantine Folders via the Web Manager

Policy Patrol includes a Web manager that allows you to view quarantined messages over the web. During installation you are given the option to install the Web manager. If you selected 'No' during installation and you want to install the Web Manager after the initial installation, you can do so from Add or Remove programs. For more instructions on this, consult paragraph 3.4 'Modifying the Policy Patrol installation'.

Policy Patrol includes two versions of the Web manager, one for users and one for Administrators. The User version only displays the messages for the user. The Administrator version allows Administrators to view all messages in the folders and provides more options. The table below highlights the differences between the two versions.

Option	User Web Manager	Administrator Web Manager
Email messages	Only user's	All
Manually add to allow/block list	Yes	Yes
Add sender address to allow/block list	Yes	Yes
Add sender domain to allow/block list	No	Yes
Add to IP allow/block list	No	Yes
Move message to other folder	No	Yes
Deliver to other recipient	No	Yes
View Message history	No	Yes
View Event history	No	Yes
Search messages	Yes	Yes

Tip

You can add a link to Outlook so that you can view the web manager directly from Outlook. To do this, create a new folder in Outlook. If you want the folder to be listed at the top, start

the folder name with a symbol, for instance @Spam. Now right-click the folder and select **Properties**. Go to the **Home page** tab and enter the link for the Policy Patrol Web manager, i.e. http://<Policy Patrol Server Name>/PolicyPatrolEmail/WebManager.aspx, where IP address is the IP address of the Policy Patrol machine. Click **OK**. Now when you click on the folder in Outlook it will automatically open up the Web manager.

The documents below will help you inform your users about how to use the Policy Patrol quarantine reports and Web Manager. Both documents are in Microsoft Word so that you can place your own logos and enter the correct Web Manager links before distributing the documents amongst your users:

Policy Patrol User Memo
(http://www.policypatrol.com/assets/pp10-usermemo.doc)

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

13.6.1 Web Manager URL

You can access the Policy Patrol Web Manager by going to http://<servername>/policypatrolemail/, where <servername> is the name of the Policy Patrol machine, for instance `http://server01/policypatrolemail`. The Web Manager link is displayed in Policy Patrol Administration > **Settings** > **Web Manager**. Instead of <servername> you can also enter the IP address of the Policy Patrol, however in that case the user will be prompted for user credentials. When the <servername> is used in the URL, Windows Integrated Authentication will be used and the user will not be asked to enter their credentials.

When users go to the Web Manager link they will automatically be directed to the User Web Manager where they can only see their own emails. When Administrators go to the Web Manager link they will automatically be directed to the Administrator Web Manager where they can see all users' emails. If you are an Administrator and you only wish to view your own emails, you must add /webmanager.aspx after the web manager link as follows: http://<servername>/policypatrolemail/webmanager.aspx, for instance `http://server01/policypatrolemail/webmanager.aspx`.

13.6.2 Web Manager Permissions

Only Policy Patrol Administrators (by default these are all members of the Administrative Group in Active Directory, or if users are selected under **<server name>** > **Security** > **User security**, only the users that have been assigned Administrator rights) will be able to access the Administrator Web Manager and view all users' emails. For more information on how to configure Policy Patrol Administrators, you can consult the paragraph 20.1.1 'User access rights'.

Users can only access the User version of the Web manager if they have been given permissions to the monitoring folder as described in paragraph 13.3. By default all users are granted view, deliver & delete rights for the Known spam and Suspected spam folders.

13.6.2.1 Quarantined Items

When you open the Web Manager or if you click on the Quarantined items link, a list of all quarantined messages will appear. For each message the sender, recipient(s), subject, date and folder is shown. To only view the messages in a particular folder, select the folder from the **Select Folder** drop-down list.

To deliver messages check the tick box next to the message(s) and click on the **Deliver** button or the **Deliver & add to Allow list** button. If you select **Deliver & add to Allow list**, the sender email address will be added to the Allow list as well as delivering the message.

To delete messages check the tick box next to the message(s) and click on the **Delete** button or the **Delete & add to Block List** button. If you select to delete messages, the messages are permanently deleted. If you select **Delete & add to Block list**, the sender email address will be added to the block list as well as deleting the message.

Further actions can be selected from the **More Actions** drop down box. The following options are available: Add IP address to allow list, Add email address to allow list, Add email domain to allow list, Deliver to other recipient(s), Move to folder, Add IP address to block list, Add email address to block list and Add email domain to block list.

You can search for messages by entering a word or email address in the search field. Policy Patrol will search the sender, recipient, subject, content, attachment name and date fields. To specify more advanced options, click on the **Advanced Search** link. You will be able to select which folder to search and to search only particular fields.

Search Field	Description
Sender:	From: and X-Sender fields
Recipient(s):	To: and X-Receiver fields (includes Cc: and Bcc: recipients)
Cc:	Cc: field
Subject	Subject of the message
Attachment	Attachment name
Date	Date the message was sent

13.6.2.2 Message History

To view the message history, click on the **Message History** link. A list will be displayed of up to the last 2000 messages processed by Policy Patrol. For each message the sender, recipient(s), subject, date and action will be displayed.

13.6.2.3 Event History

To view a list of Policy Patrol events, click on the **Event history** link. A list of recent events will be displayed. For more information on the types of events that are displayed, consult chapter 14 'Logs.'

13.6.2.4 Allow List

Enter the email address or domain that you wish to add to the allow list and click **Submit**. If you wish to add a domain, just enter the part after the @ sign, for instance `company.com`. This will include info@company.com and sales@company.com, but not newsletters@news.company.com.

If you wish to include these email addresses as well, enter `*company.com`. In view of processing times however, try not to add too many * to the white list.

13.6.2.5 Block List

Enter the email address or domain that you wish to add to the block list and click **Submit**. If you wish to add a domain, just enter the part after the @ sign, for instance `spammer.com`. This will include info@spammer.com and sales@spammer.com, but not newsletters@news.spammer.com. If you wish to include these email addresses as well, enter `*spammer.com`. In view of processing times however, try not to add too many * to the block list. Remember that spammers continually change and/or spoof their email address so adding many entries to the block list is not an effective way to block spam.

Chapter 14

Logs

Policy Patrol Email includes detailed logs that allow you to track individual messages, troubleshoot policies, test the effectiveness of certain spam filtering techniques as well as track which users took which actions.

14.1 History

The History view includes an overview of up to the last 5000 messages processed by Policy Patrol. By default the last 100 messages will be shown. To display a larger number of messages, select the number of messages to be displayed from the drop down list in the top right corner. The list is continually updated and displays the date/time processed, sender, recipient(s), subject, size of the message, and the action that was taken.

The icon for the message indicates which action was taken, i.e. delivered, moved to folder, deleted or redirected. Below is a list of the different icons and the corresponding actions.

Icon	Action
	Delivered
	Moved to Folder
	Deleted
	Redirected to an alternate recipient

To see only emails for which a certain action was taken, click on the drop down list next to the Filter icon  and select the action to display.

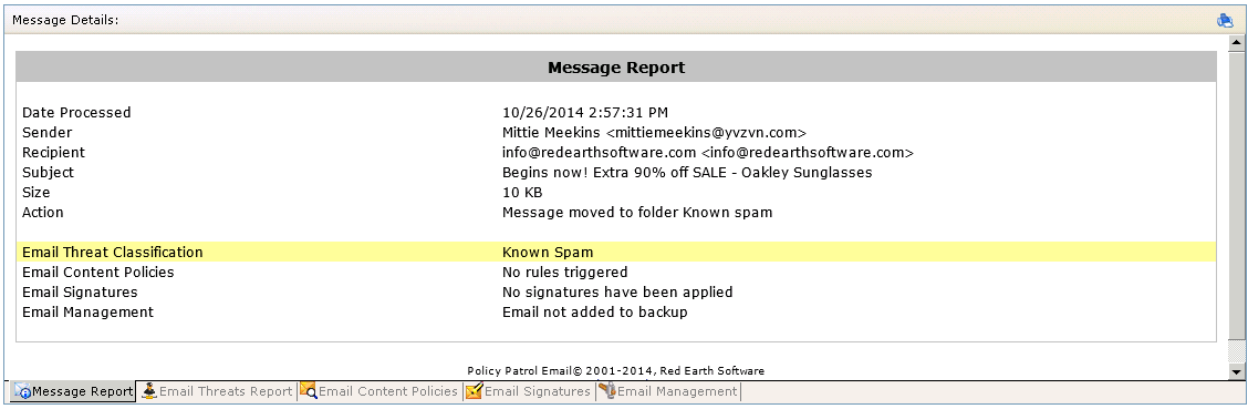
You can add the senders of a particular message to filters by selecting the relevant message(s), right-clicking and selecting **Allow list** or **Block list**. You will then have the option to add the sender email address, email domain or IP address to the allow list or block list.

Since the message history list is continually updated, if you want to preserve the list of messages you can select the relevant messages, right-click and select **Export selected rows**. The information will be saved to a txt file that you can import as a Tab delimited file in Microsoft Excel.

To view the details of the message, select the message in the top pane. The bottom pane will display the reports for the message. The following reports are shown: Message Report, Email Threat Report, Email Content Policies Report, Email Signature Report and Email Management Report.

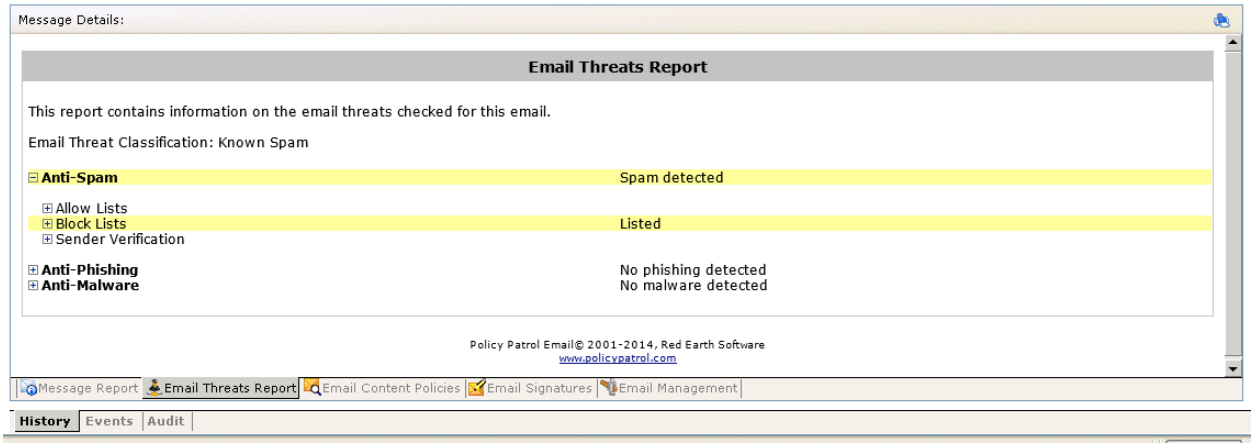
14.1.1 Message Report

The Message Report includes the details of the message and the action that was taken by Policy Patrol. It also lists whether a threat was detected, any policies triggered, any email signatures were added and whether any email management options applied. If affirmative, the option will be highlighted.



14.1.2 Email Threats Report

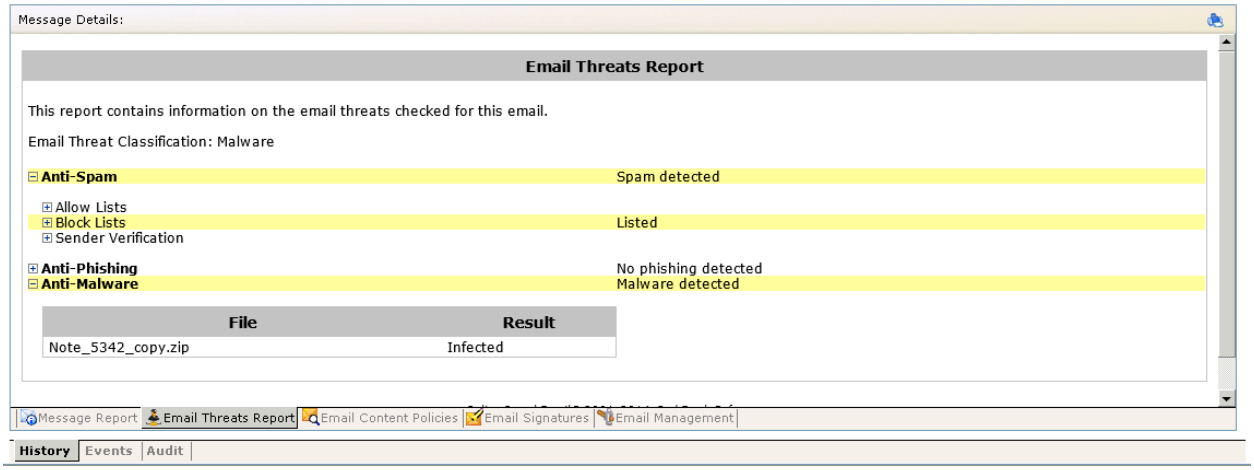
The Email Threats Report includes information on the results found for each email threat: Spam, Phishing and Malware. If a threat was found, the threat will be highlighted. Click on the plus signs to find the triggering event for the message. For instance for Anti-Spam, if the Block list is highlighted, this means that the sender of the message was found to be on one of the block lists. Click on the plus sign to find out which list the sender was listed on. If any words in the message were found in the block list or allow list, the individual words and their score will be listed in the report. To print the report, click on the **Print** icon in the top right hand corner.



Anti-Spam	Spam detected
Allow Lists	
Block Lists	Listed
Email	Not on email block list
Words	Not on word block list
IP Address	Not on IP block list
Countries	Not on country block list
Character Sets	Not on character set block list
DNSBL	Listed
Sender	On DNSBL
DNSBL	Not enabled
CBL	Not enabled
SpamCop	Not listed
Mail Police (Block)	Not listed
Mail Police (Adult)	Not enabled
Mail Police (Dynamic)	Not enabled
AHBL	Not enabled
UCEProtect	Listed
SORBS	Not listed
MegaRBL	Not listed
Blocklist.de	Not listed
SURBL	Not listed
Sender Verification	

If phishing was detected, Anti-Phishing will be highlighted and the list will be shown.

If malware was found in the message, Anti-Malware will be highlighted. Click on the plus sign to see the name of the malware.



14.1.3 Email Content Policies Report

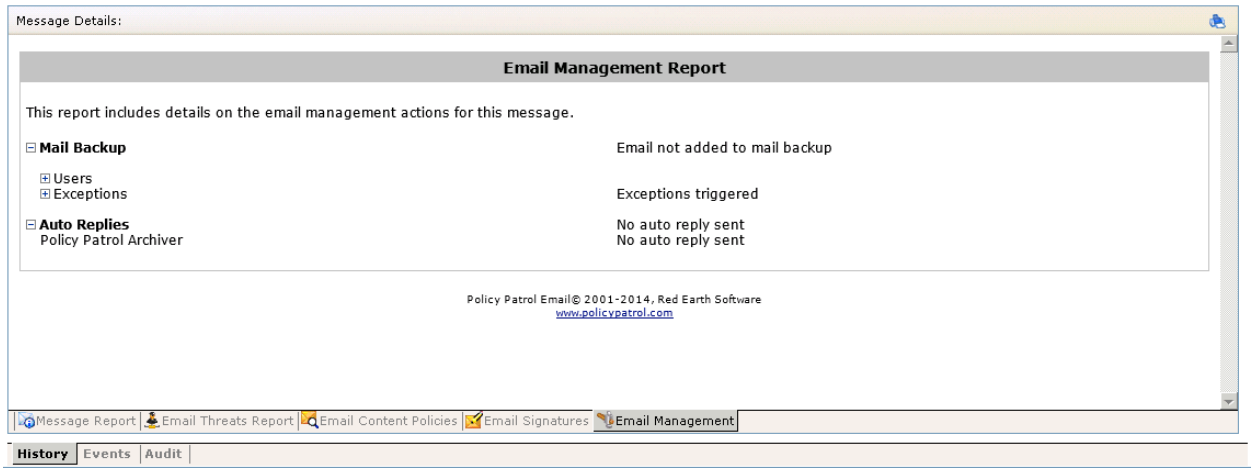
The Email Content Policies Report includes a list of all policies that were processed and whether they triggered for the message. Triggered policies will appear highlighted in the report. Each recipient will be listed separately, since different email policies can be applied for each recipient. To print the report, click on the **Print** icon in the top right hand corner.

14.1.4 Email Signatures Report

The Email Signatures Report will show any email signature policies that have been processed and if applicable, have been applied. Each recipient will be listed separately, since different email signatures can be applied for each recipient.

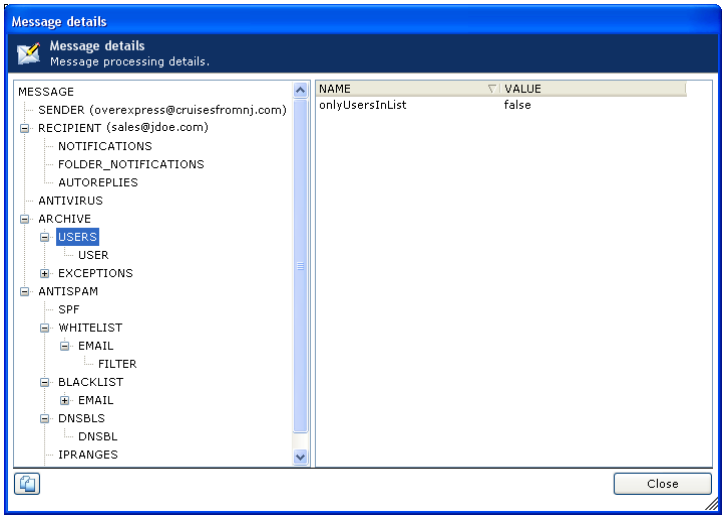
14.1.5 Email Management Report

The Email Management report will show whether the message was backed up and whether an auto reply was sent for the message.



14.1.6 Viewing Details

Although most of the message details are already available in the Message reports, it is possible to view further details for the message by right-clicking the message and choosing **Details**. The details dialog will include information on the results of each spam filtering method and policy that was processed and if relevant will list any words found and their score. To copy the complete details to a text file, click on the **Copy** button in the bottom left hand corner.



14.2 Event History

The event history displays a list of the following events:

- Folder agent triggered
- IP Range rejected a message (Dropped SMTP connection)
- DNSBL rejected a message (Dropped SMTP connection)
- Email blocklist rejected a message (Dropped SMTP connection)
- IP Range blocklist rejected a message (Dropped SMTP connection)
- Recipient verification rejected a recipient

- Address harvesting protection dropped an SMTP connection.
- Sender DNS lookup failed and dropped an SMTP connection.
- Sender Policy Framework rejected a message (Dropped SMTP connection).

It is also possible to add IP addresses to the block lists straight from the Event History view.

14.1 Audit Logs

The Audit Logs show certain user actions, including delivering and deleting messages and adding addresses to the allow list and block list. The following actions from the Web Manager and Administration console are recorded in the Audit log:

- Deliver
- Move
- Delete
- Allow list (email)
- Allow list (IP)
- Block list (email)
- Block list (IP)

In addition, any challenge/response verifications that have been submitted via the challenge/response website will also be logged in the Audit Logs.

Chapter 15

Email Management

Policy Patrol includes several tools for managing email, including Mail backup, Reporting, Auto replies and a POP3 downloader. This chapter explains how to configure auto replies and the POP3 downloader. Mail backup and Reporting are described in the following chapters.

15.1 Auto Replies

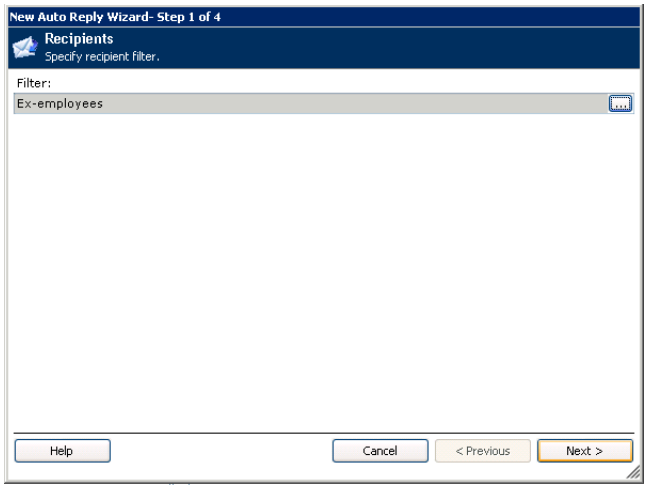
Policy Patrol includes the possibility to configure auto replies. This allows you to send auto replies to web forms and information requests, but also to send auto replies when messages are sent to email addresses of ex employees.

To configure a new auto reply:

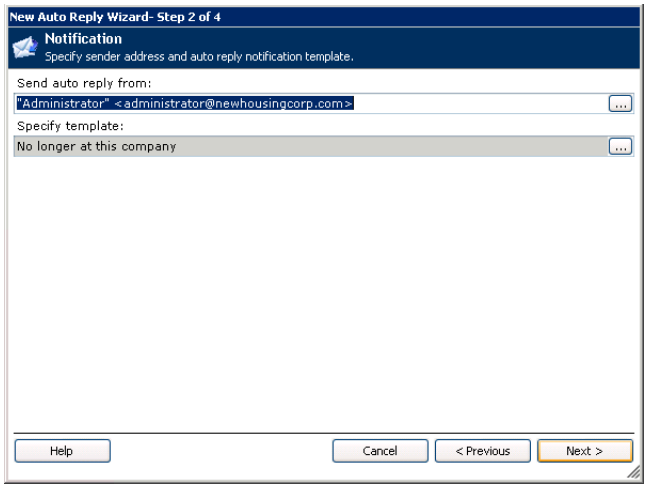
1. Go to **Email Management** > **Auto Replies**. Click **New**.

2. Click **Next** in the Welcome screen.

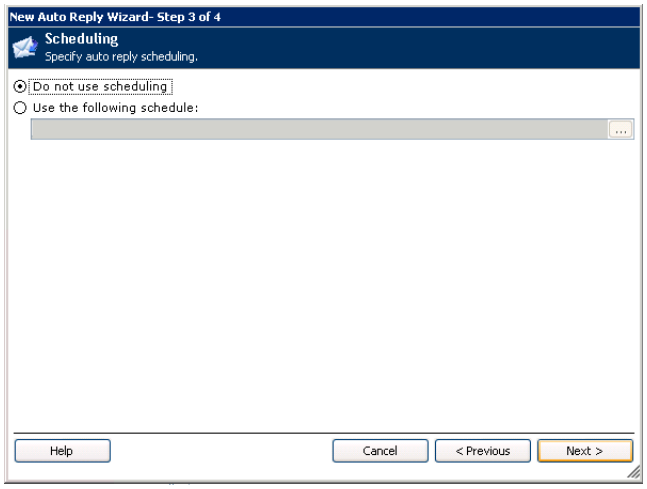
3. Select the recipient filter you wish to send the auto replies to by clicking on the **..** button. Select the filter from the list. If you wish to create a new filter, click on the **New** button above the available filters list. When you are done, click **OK**. Click **Next**.



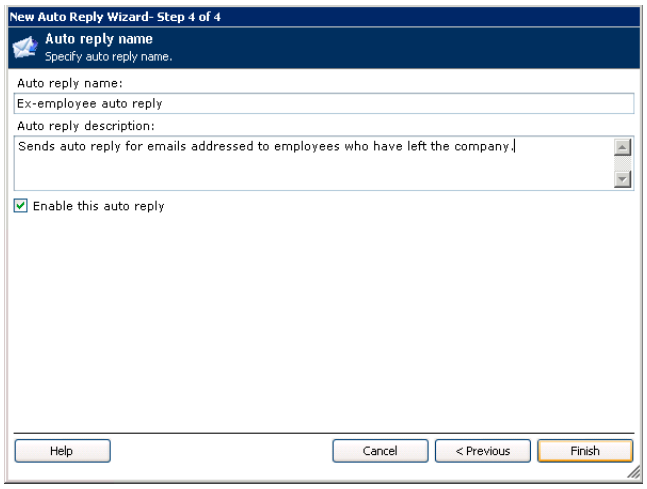
4. In 'Send auto reply from:' enter the email address to be included in the From address. Alternatively select a user by clicking on the **Browse** button. Now select the notification template to be used for the auto reply by clicking on the **..** button. Select the template from the list. If you wish to create a new template, click on the **New** button above the available templates list. When you are done, click **OK**. Click **Next**.



5. Specify whether you wish to use scheduling. If you do not wish to use scheduling, select **Do not use scheduling**. If you wish to schedule the auto replies, select **Use the following schedule** and select the schedule from the list. If you wish to create a new schedule, click on the **New** button. Click **Next**.



6. Enter a name and description for the auto reply. If you wish the auto reply to be enabled, leave the option **Enable this auto reply** ticked. Click **Finish**.



To edit the auto reply, select the auto reply in the list and click on the **Edit** button. To delete the auto reply, select the auto reply in the list and click on the **Delete** button. If you wish to rename the auto reply, select the auto reply in the list, right-click and choose **Rename**.

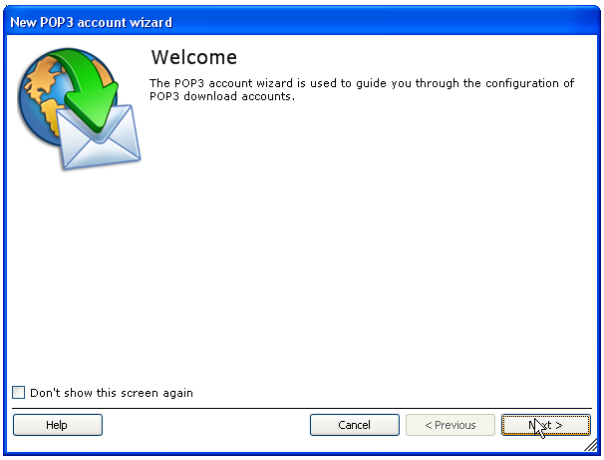
Tip

You can use Policy Patrol to automatically send replies to web forms by creating a different email address for each web form. If you also want to perform automated follow up after a specified time, you must use the Email Content Policies. For more information on how to do this, please consult the document 'Email Management with Policy Patrol' which is available for download from www.policypatrol.com/documentation.

15.2 POP3 Downloader

To create a new POP3 account to download messages from, follow the next steps:

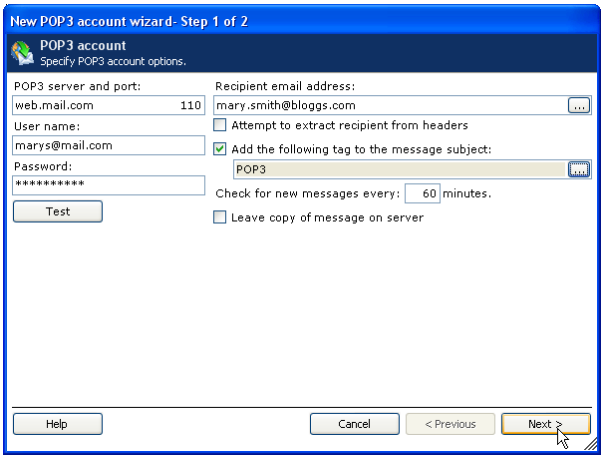
1. Go to **Email Management** > **POP3 Downloader** and click **New**.
2. In the Welcome screen, click **Next**.



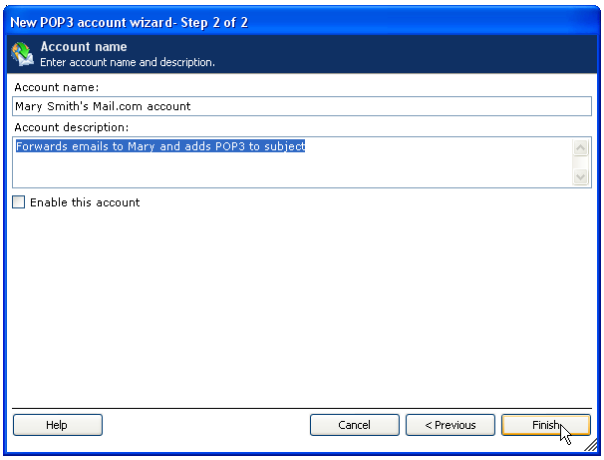
3. Enter the address of the POP3 server. Leave the Port at 110 unless you are using a different port. Enter the user name and password for the POP3 account. Click **Test** to verify the connection. Now specify to which email address the POP3 mails should be forwarded. If you wish to download email for multiple recipients, you can select the option **Attempt to extract recipient from headers**. If Policy Patrol does not find a recipient, the email will be forwarded to the default recipient email address.

   Optionally you can add a tag to the message subject for messages that were downloaded via POP3. To do so, enable the option **Add the following tag to the message subject**, press on the **...** button and select the tag template to be used.

   Finally, specify how often to check for new messages and whether you wish to leave a copy of the mail on the server. When you are done, click **Next**.



4. Enter a name and a description for the POP3 account. Click **Finish**.



To edit an existing POP3 account, select the account in the list and click on the **Edit** button.

To start downloading emails before the scheduled time, right-click the account and select **Poll now**.

Note

Policy Patrol will process POP3 messages in the same way as SMTP messages. The only difference is that it is not possible to drop the SMTP connection. If this option is selected in anti-spam actions, the message will be deleted instead. A Sender Policy Framework check can be done on the reply to: email address.

Chapter 16

Mail Backup

Policy Patrol can save a backup of emails into a SQL Server database. Emails can be retrieved from the Administration console.

16.1 Mail Backup

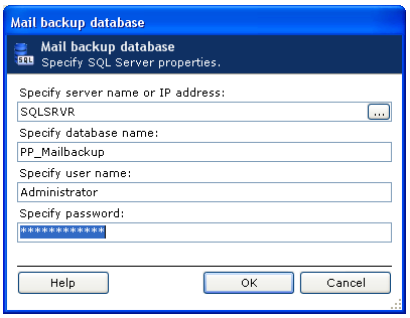
Mail backup is a useful tool for providing an additional backup method and allowing users to retrieve individual messages. If disaster strikes, your last Exchange backup tape is not likely to be any more recent than yesterday's emails. However, with Mail backup enabled, Policy Patrol will provide you with a backup of all emails sent and received right up until the last minute. In this way you will never have to lose a single email again. Policy Patrol allows you to easily search and restore messages from the Administration console.

> **Note**
>
> Microsoft SQL Server does not have to be installed on the same machine as Policy Patrol.

16.2 Enabling Mail Backup

You can enable Mail backup by following the next steps:

1. Go to the **Email Management > Mail Backup** node.
2. Select the option **Enable mail backup**.
3. Enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically create the database for you. If you do not have SQL Server, you can also specify a SQL Server Express database. Click **OK**. Each message that is sent and received will now be copied into the database.



Tip

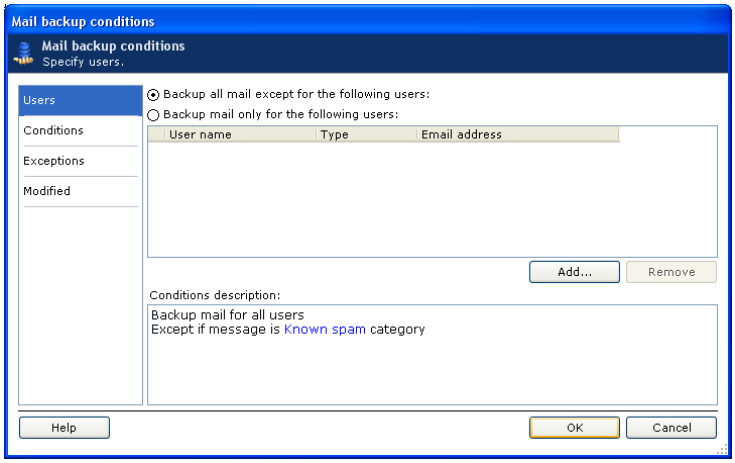
If you do not have SQL Server, you can also use SQL Server Express for Policy Patrol Mail backup.

16.3 Mail Backup Conditions

Policy Patrol allows you to specify which users and/or emails you wish to include in the Mail backup database. To specify conditions, click on **Configure mail backup conditions**. A tabbed dialog will appear with the following options: Users, Conditions, Exceptions and Modified. Each tab is described below.

16.3.1 Selecting Users for Mail Backup

To backup mails for selected users, click on **Users** in left column and select **Backup all mail except for the following users** or **Backup mail only for the following users**. To add users to the list, click on **Add**.

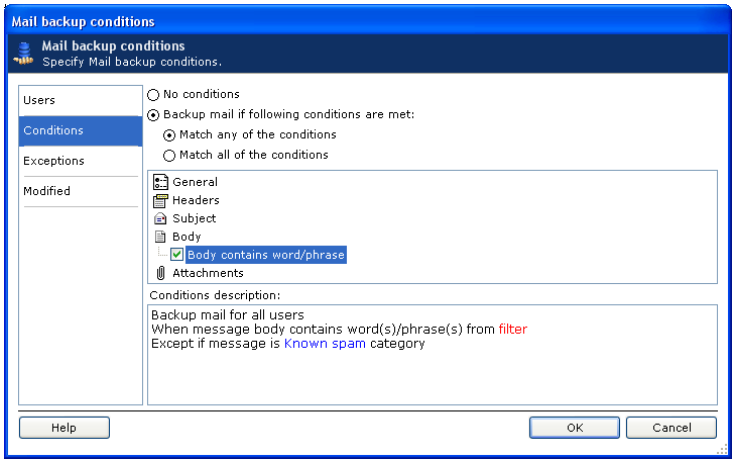


16.3.2 Specifying Mail backup Conditions

To specify particular messages to be copied into the database, click on **Conditions** in the left column. Here you can specify which conditions should be met for the message to be saved into the database. If all messages should be copied, leave **No conditions** selected. If you only want

certain messages to be archived, select **Backup mail if following conditions are met**. The different conditions are sorted into the following 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 want to archive messages that contain certain words or are from a specified sender, 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 only archive messages to certain recipients that have an attachment.



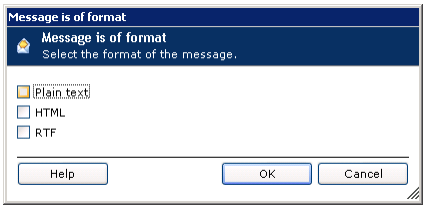
Available conditions:

- **General**

  ☑ **Message is encrypted**: This condition checks whether a message is encrypted.

  ☑ **Message is digitally signed**: This condition checks whether a message is digitally signed.

  ☑ **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.

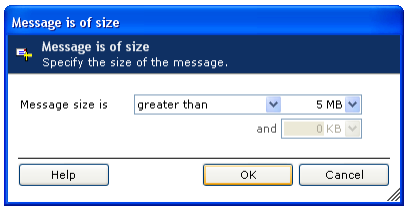
☑ **Message is of priority/importance**: Specify whether the message should be of High, Normal and/or Low priority.



☑ **Message is of sensitivity**: Specify whether the message should be Normal, Personal, Private and/or Confidential.



☑ **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 policy 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 policy 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 policy will not trigger for messages of 2 MB and 3 MB and any size in between.

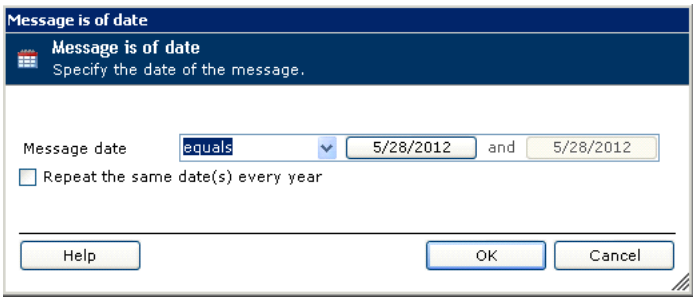


Note

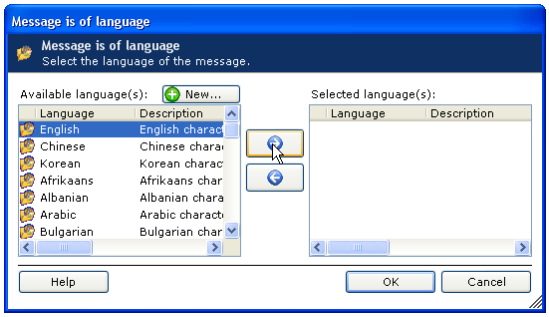
Policy Patrol counts the actual message size as received by the mail server. This can be a little different from the message size as received by Outlook or the message size of a Quarantined message in Policy Patrol. There are a number of reasons for this, such as different encoding of the email or attachment, 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 **equals**, the policy will only trigger on the selected date. If you select **is before** or **is after**, the policy will trigger before or after

the selected date (date itself will not be included). For instance, if you specify that a policy should trigger for dates before October 1st, the policy will trigger for messages sent on or before September 30th, but not on October 1st. If you select **between** or **not between**, this will include the two values. For instance, if you select **between** 5th and 7th September, the policy will trigger for messages sent on 5th, 6th and 7th September. If you select **not between** 5th and 7th September, the policy will not trigger for messages sent on 5th, 6th and 7th September. Check the option **Repeat the same date(s) every year** if you wish the policy to trigger on the specified days of the month, irrespective of the year.



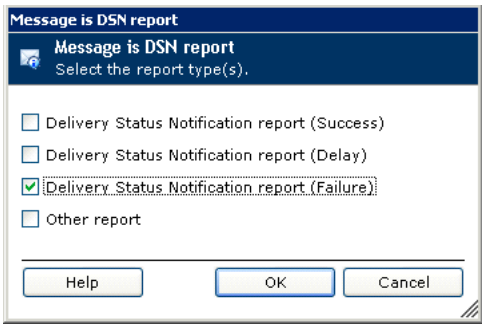
☑ **Message is of language**: Specify whether the message should use a certain language. Select the language in the left pane and clicking the **>** button. To edit a configured language, right-click the language and select **Edit**. To create a new language, click on the **New** button. When you are done, click **OK**. Languages can be configured in **Settings** > **Languages**.



☑ **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 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.

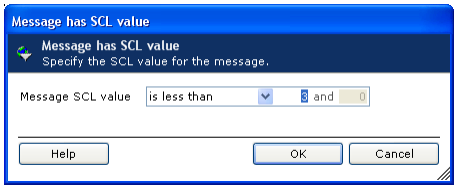
☑ **Message is DSN report**: Specify whether the message should be a Success, Delay and/or Failure notification, or Other report (report without status code).



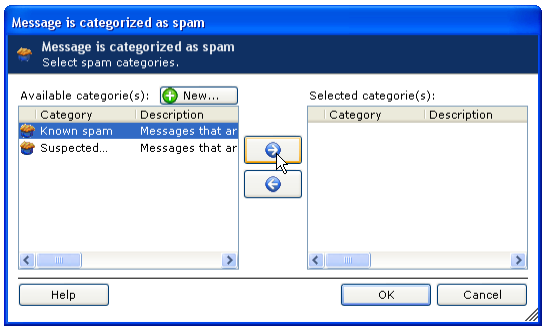
Note

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 Policy Wizard.

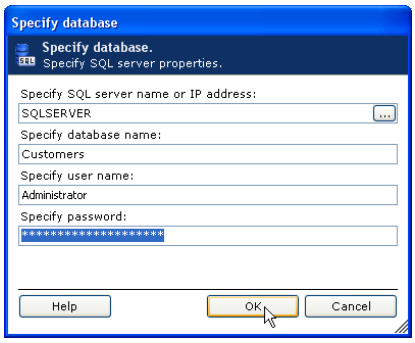
☑ **Message has SCL value:** By checking this option Policy Patrol will check to see if the message has an SCL value within the specified range. The SCL value can be from 1-9, with 1 indicating a legitimate message and 9 indicating a spam message. Note that this feature requires Exchange 2003 or higher.



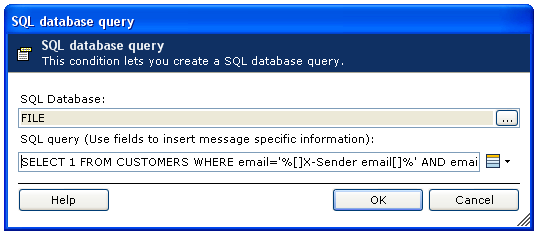
☑ **Message is categorized as spam:** This condition allows you to apply policies to messages that have been classified by certain threat classifications. If you only want to handle spam using the Email Content Policies (for instance if you want to handle spam differently per user), you can simply configure the action 'Accept message' in the threat classification and select this condition to trigger the appropriate policy.



☑ **Message matches SQL database query:** This condition allows you to look up information in a SQL database and search for this information in any message or user field. For instance you could use this condition to trigger a policy only when senders or recipients are found in the database. Firstly you need to specify the SQL database settings by clicking on …



Enter the SQL Server name or IP address, or click on **...** to browse to the machine. Enter the database name and enter the user name and password for accessing the database. Click **OK**.



Now you must enter the SQL query in the following format:

SELECT 1 FROM [SQL_table_name] WHERE [column_name]=%[]Message field[]%

Where:

[SQL_table_name] = name of the table in SQL Server to look up information from

[column_name] = name of the table column where you want to look up information

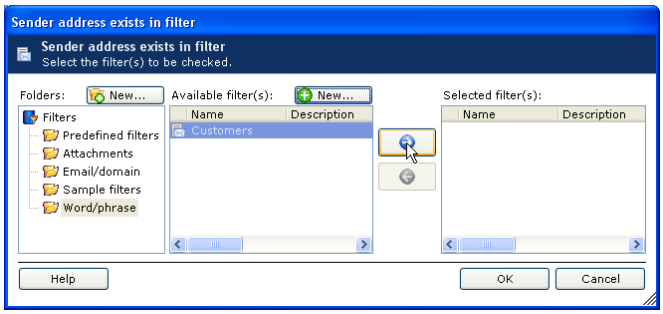
%[]Message field[]% = Message field that you want to match in the SQL table column

For instance, you have a SQL table called CUSTOMERS and in the 'Email' column you have listed all your customers' email addresses. To trigger a policy that applies only to emails sent to email addresses in the CUSTOMERS table, excluding those entries in the database without an email address, you must enter the following query:

```
SELECT 1 FROM CUSTOMERS WHERE Email='%[]X-Receiver email[]%' AND email <> ''
```

- **Headers**

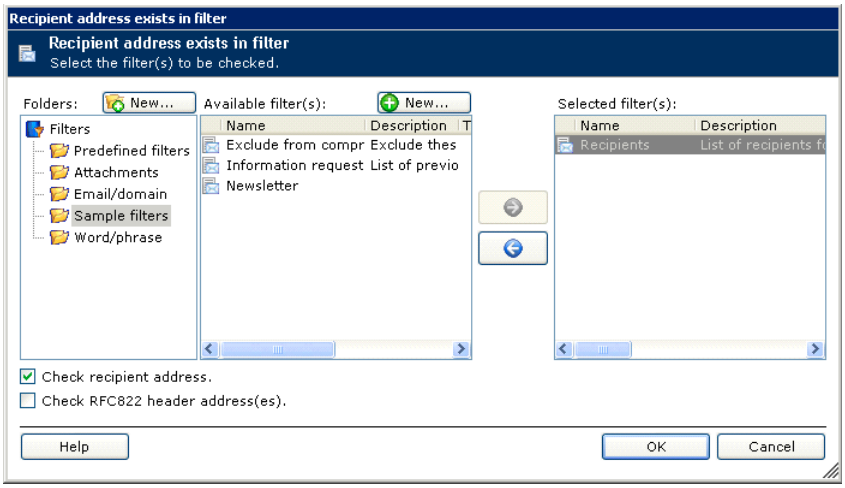
☑ **Sender address exists in filter**: Select the Email/domain filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol will check the From: and X-Sender fields for the configured address(es).



Note

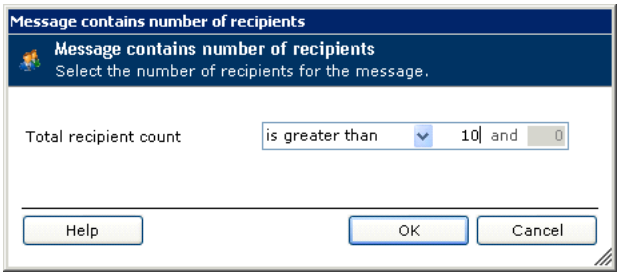
The predefined filters folder contains the Email block list and Email allow list filter. These lists are configured from Anti-spam > Block/Allow. If you wish to handle spam messages via the policies you can select these filters if you wish.

☑ **Recipient address exists in filter**: Select the Email/domain filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. If you wish Policy Patrol to check the X-Receiver field, select the option **Check recipient address**. If you wish to check the To: and Cc: fields, enable the option **Check RFC822 header address(es)**.

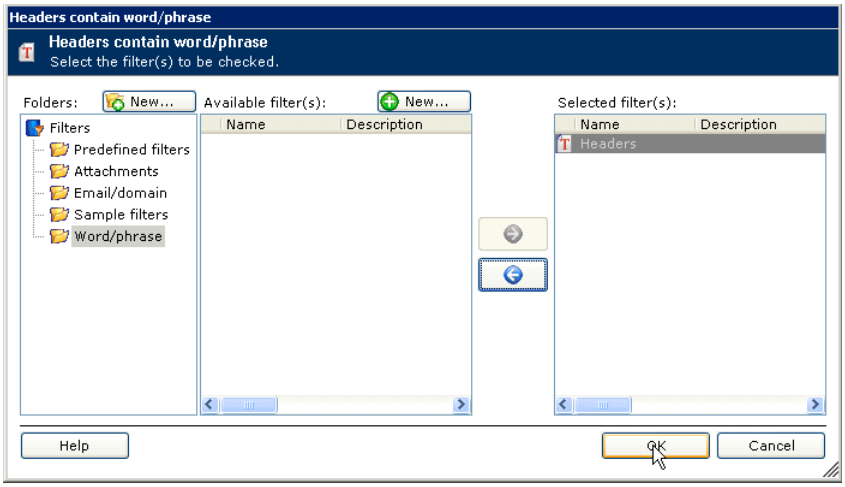


☑ **Message contains number of recipients**: Specify whether the total recipient count (the number of recipients in the To: and Cc: fields) should be equal to or greater than, less than, between or not between a certain value. If you select **is greater than** or **is less than**, the value itself will not be included. For instance, if you specify that a policy should trigger when there are more than 2 recipients, the policy will trigger for messages with 3 or more recipients. If you select **is between** or **is not between**, this will include the two values. For instance, if you select **is between** 2 and 4 recipients, the policy will trigger for messages with 2, 3 and 4 recipients. If you select **is not between** 2 and 4

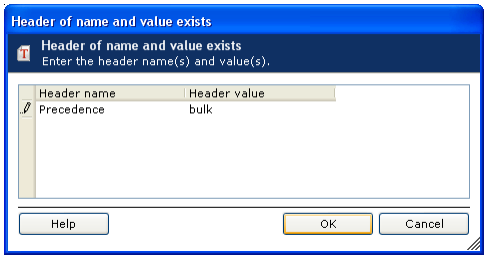
recipients, the policy will not trigger for messages with 2, 3 and 4 recipients. Policy Patrol cannot count bcc: recipients. Distribution lists will be counted as one recipient.



☑ **Headers contain word/phrase**: Select the filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol will search all headers for the word(s) in the filter.



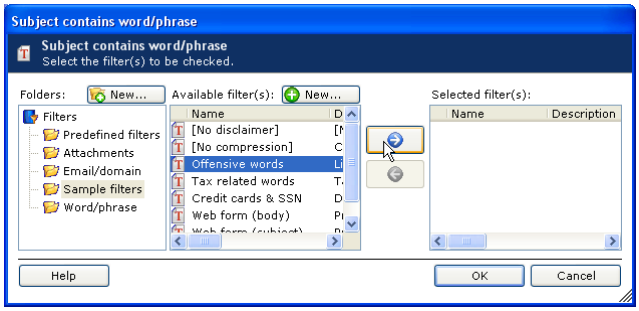
☑ **Header of name and value exists**: Enter the header name and value that Policy Patrol must search for.



- **Subject**

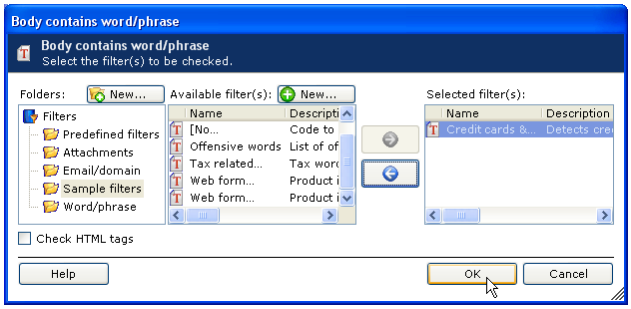
☑ **Subject is missing or empty**: Check this option if you wish the policy to trigger when a message has an empty subject or no subject field at all.

☑ **Subject contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list.



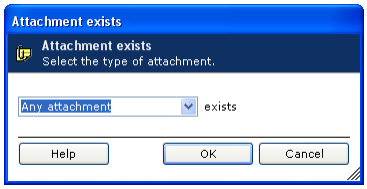
- **Body**

☑ **Body contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folders list. If you wish to check the HTML source code, check the option **Check HTML tags**. This can be useful if you want to check for scripts by searching for the `<SCRIPT>` tag. If you wish to check normal text, do not select this option since it will produce unwanted results.



- **Attachment**

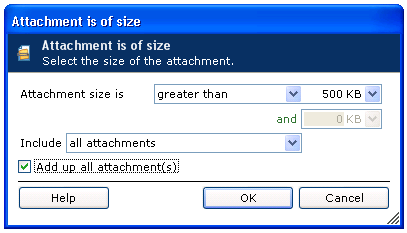
☑ **Attachment exists**: Select whether you wish to check for **any attachment**, **inline attachment** (embedded pictures) or **standard attachment** (files that have been attached to the message).



Note

Inline attachments are pictures or objects that have been inserted in the email message itself. Non-inline attachments are files that have been attached to the message.

☑ **Attachment is of size**: Specify whether the attachment should be **greater than**, **less than**, **between** or **not between** certain values. By default each attachment to the message is counted separately. So if you have a policy that triggers when an attachment is greater than 1 MB, the policy will not trigger for a message that includes two attachments of 550 KB each. If you wish to check the total size of attachments to the message, you must select the option **Add up all attachments**. Specify whether you wish to check for **all attachments**, **inline attachments only** (embedded pictures) or **standard attachments only** (files that have been attached to the message).



☑ **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 CLSID extension.

Attempt to verify attachment extension: Policy Patrol can verify over 100 file types. A list of files that Policy Patrol can verify is found in **Settings** > **Attachment Maps**. For

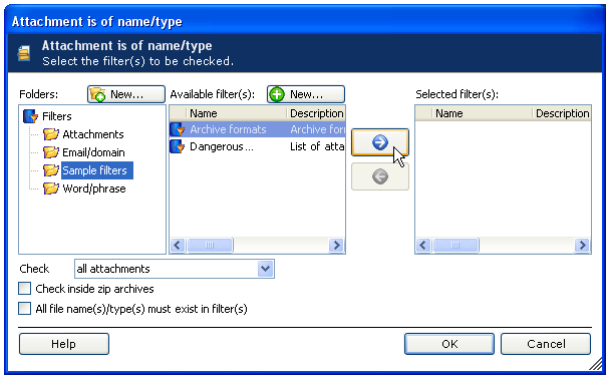
instance, if a user tries to circumvent a policy blocking exe files and renames the `virus.exe` file to `virus.doc`, Policy Patrol will block this file since it can verify that the file is not a doc file.

Check for binary text files: 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.

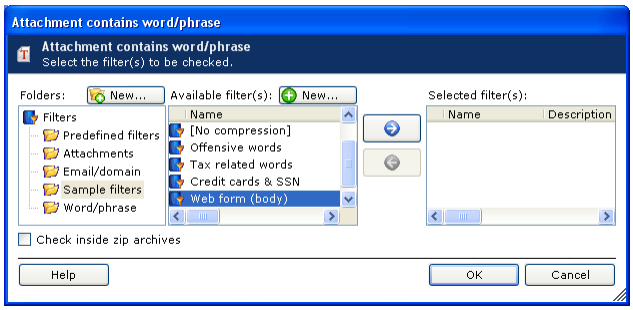
☑ **Attachment is of name/type**: Select the attachment filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Specify whether you wish to check for **all attachments**, **inline attachments only** (embedded pictures) or **standard attachments only** (files that have been attached to the message). If you want Policy Patrol to check attachments within zip files, check the option **Check inside zip archives**. If you wish all file names/types to exist in the filter in order to trigger the condition, check the option **All file name(s)/type(s) must exist in filter(s)**.

Note

If you create a policy that allows only safe attachments to be received, you must check the option **All file name(s)/type(s) must exist in filter(s)**. If you did not check the option, messages with at least one safe attachment would be let through no matter whether the other attachments were safe. Note: do not check the option **All file name(s)/type(s) must exist in filter(s)** when you are blocking dangerous attachments. Checking this option would mean that the message would not be blocked if it contained safe attachments as well as dangerous attachments.



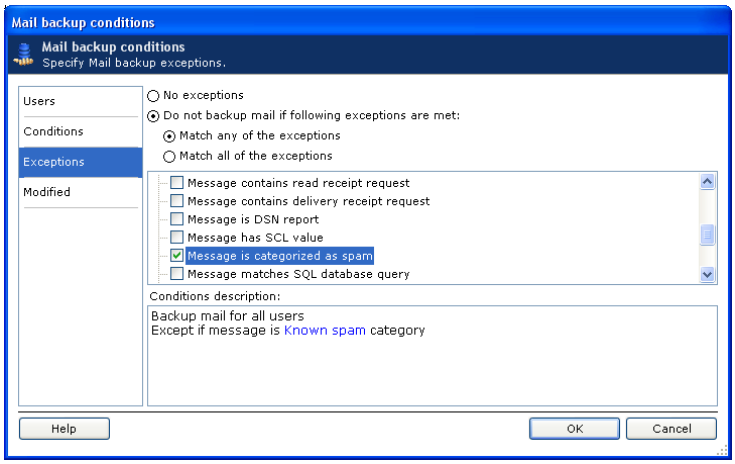
☑ **Attachment contains word/phrase**: Select the word/phrase filter(s) to be checked by browsing to the correct folder and selecting the filter(s) in the left pane. Now click on the ➔ button. To edit a configured filter, right-click the filter and select **Edit**. To create a new filter, click on the **New** button above the available filters list. To create a new folder, click on the **New** button above the folder list. Policy Patrol can check text and html documents. If you want Policy Patrol to check attachments within zip files, check the option **Check inside zip archives**.



☑ **Message contains number of attachments**: Specify whether the number of attachments must equal or be greater than, less than, between or not between a certain value. If you select **is greater than** or **is less than**, the value itself will not be included. For instance, if you specify that a policy should trigger when there are more than 2 attachments, the policy will trigger for messages with 3 or more attachments. If you select **is between** or is **not between**, this will include the two values. For instance, if you select **is between** 2 and 4, the policy will trigger for messages with 2, 3 and 4 attachments. If you select **is not between** 2 and 4, the policy will not trigger for messages with 2, 3 and 4 attachments. Specify whether you wish to check for **all attachments**, **inline attachments only** or **standard attachments only**.

16.3.3 Specifying Mail Backup Exceptions

To exclude particular messages from being archived, click on **Exceptions** in the left column. Here you can specify which messages should be excluded from the archive. If all messages should be archived without any exceptions, leave **No exceptions** selected. To specify particular messages to be excluded from the archive, click on **Exceptions** in the left column. For instance if you wish to exclude spam from the archive, you can do so by selecting the exception **Message is categorized as spam**. To specify exceptions, enable the option **Do not backup mail if following exceptions are met**. The options will now be the same as in the Conditions dialog (see previous paragraph).



Tip

To exclude spam and malware from the archive, select **Do not archive messages if following exceptions are met**, go to 'General' and select the exception **Message has email threat classification.** Select the threat classification that you want to exclude from the archive and click **OK**.

16.4 Message Retrieval

The Administrator can search & restore emails directly from the Administration console. Various options are available to search on, for instance sender or recipient addresses, subject or date and attachment name.

The following fields are available for searching:

Sender: In this field you can enter the sender email address that you wish to retrieve emails for. This will search for the address in the From: field as well as the X-Sender field. You can either enter the complete email address or only the domain.

Recipient(s): In this field you can enter the recipient email address that should appear in the To: field or in the X-Receiver field (this includes cc and bcc fields as well) of the message. You can either enter the complete email address or only the domain.

Cc: In this field you can enter the recipient email address that should appear in the Cc: field of the messages. You can either enter the complete email address or only the domain.

Subject: Enter the words or phrases that should be in the subject of the email. If you wish to search for a combination of words you can use the operators AND, OR and AND NOT in your search. If you are using operators you must include the words in quotes. For instance, if you want to search for emails that reference prices in 2005, you must enter "prices" AND "2005". If you want to search for the year 2005 or 2004, you must enter "2005" OR "2004". If you wish to search for all messages that reference prices apart from 2003 prices, enter "prices" AND NOT "2003". In this field you can use a * wildcard, but only at the end of your word/phrase, i.e. 2005* would include all numbers that start with 2005.

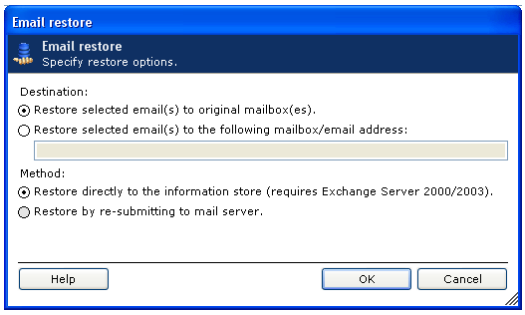
Content: Enter the words or phrases that should be in the subject of the email. If you wish to search for a combination of words you can use the operators AND, OR and AND NOT in your search. If you are using operators you must include the words in quotes. For instance, if you want to search for emails that reference prices in 2005, you must enter "prices" AND "2005". If you want to search for the year 2005 or 2004, you must enter "2005" OR "2004". If you wish to search for all messages that reference prices apart from 2003 prices, enter "prices" AND NOT "2003". In this field you can use a * wildcard, but only at the end of your word/phrase, i.e. 2005* would include all numbers that start with 2005.

Attachment: Here you can search for an attachment name that should be attached to the email, e.g. pricelist.doc. If you enter *.* or * in this field, the search will include all messages with attachments, no matter which name. In this field you can use a * wildcard, but only at the

end of your word/phrase, i.e. `price*` would include all attachments starting with the word price, for instance pricelist.doc, prices2005.htm and price list.xls.

Date: If you wish to search for emails after a specific date, tick the Start checkbox and select the start date. If you wish to search for emails before a specific date, tick the End checkbox and select the end date. If you wish to find emails between certain dates, tick both the Start and End checkboxes and select the start and end date.

After searching for and locating the required messages you may select to **Restore**, **Delete** or **View** the selected message(s) by clicking on the appropriate button. When you select **View**, you will be able to see the entire message and any attachment(s). When you click on the **Restore** button a dialog will pop up asking you to select the restore destination & method.



Restore Destination: You can select to restore the selected email(s) to the original mailbox(es), or you can select to restore to an alternative mailbox or email address.

Restore Method: You can select to restore directly to the information store or by resubmitting to the mail server.

- To restore directly to the information store, select **Restore directly to the information store**. The email(s) will be placed in the 'Policy Patrol restored emails' folder of the mailbox that you specified. The date of the message will be kept. This option is only available if you have installed Policy Patrol on an Exchange Server machine, and you are accessing Policy Patrol on the server machine (not via Remote Administration). Note that in order to restore to the information store, you must enable **Update Outlook Sent Items with email modifications** in System configuration > Email modifications (see paragraph 19.3.3).

- To resend the message, select **Restore by re-submitting to mail server**. The message(s) will be resent and will appear in the user's inbox. Note that a new date and time will be applied to the message.

If you wish to export messages you can do so by right-clicking and selecting **Export selected items**. The message list will be exported to a text file.

Chapter

17

Reporting

Policy Patrol includes extensive reports providing details on spam filtering, monitoring, virus scanning, email traffic, policy processing and attachments. This chapter describes how to configure reporting, run reports and how to automatically generate and email reports.

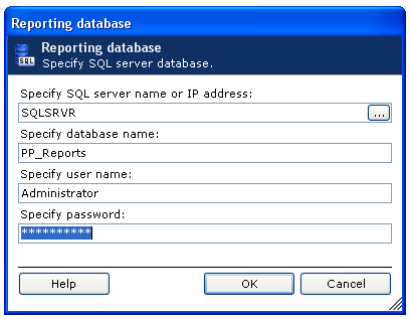
17.1 Enabling Reporting

To enable reporting in Policy Patrol, follow the next steps:

1. Go to **Email Management** > **Reporting**.

2. Select the option **Enable reporting**.

3. Enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically create the database for you. If you do not have SQL Server, you can also specify an MSDE or SQL Server Express database. Click **OK**. Each message that is sent and received will now be included in the reports.



Note

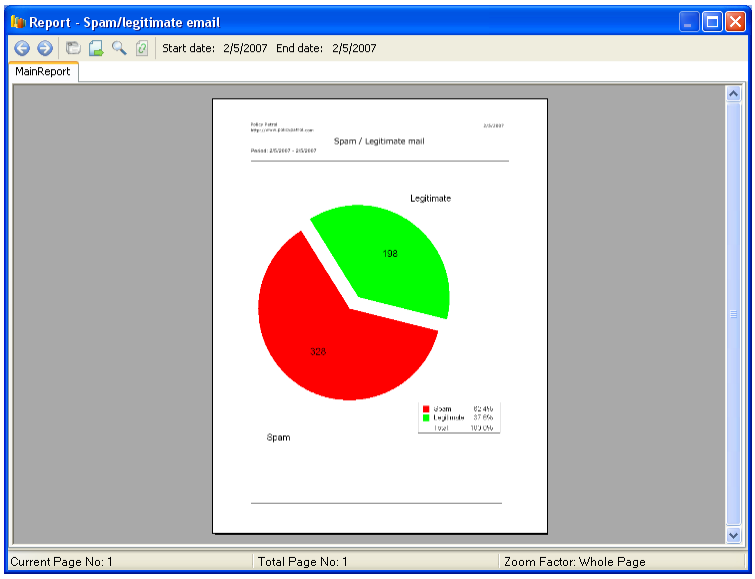
Microsoft SQL Server does not have to be installed on the same machine as Policy Patrol.

Tip

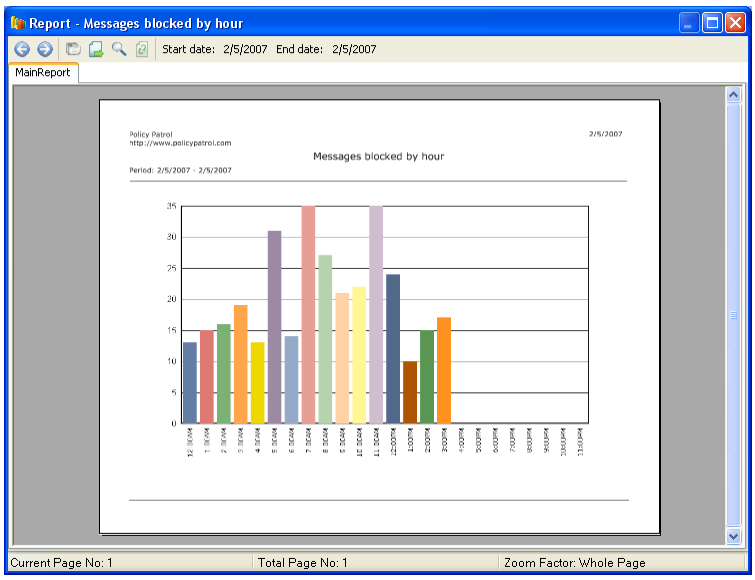
If you do not have SQL Server, you can also use MSDE or SQL Server Express.

17.2 Running Reports

To run a report, select a report in the list and click **Run**. The report will be displayed.



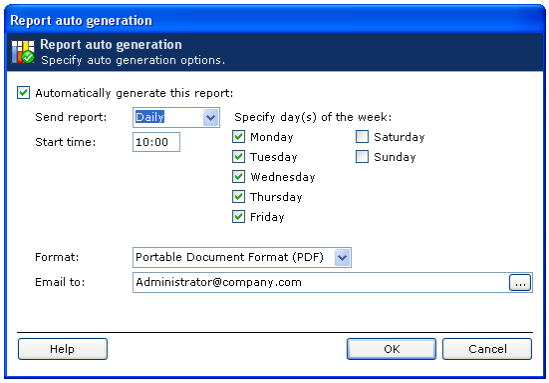
For each report you can apply filters, such as date range and if applicable, user or policy. To change the dates for the reports, click on the Start or End date in the toolbar and select the appropriate date in the calendar.



To select specific users, click on **(all users)** in the toolbar. A dialog will pop up allowing you to select and deselect users. To select specific policies, click on **(all policies)** in the toolbar. A dialog will pop up allowing you to select and deselect policies. These options will only be available for certain reports.

17.3 Auto Generating Reports

If you want Policy Patrol to automatically generate and email reports, select the report in the list and click on **Auto Generate...**. Tick the option **Automatically generate this report** and select Daily, Weekly or Monthly from the drop-down list. Enter the time that the report should be sent and select which days of the week the report should be generated. You can select the format in which the report should be sent, including pdf, xls, doc and rtf. Enter the email address where the report should be sent to. Multiple email addresses should be separated by a semi colon (;).



Note

The top spam senders, top spam receivers, top spam domains and top spam IP addresses reports can only be run on a daily basis.

17.4 Available Reports

Policy Patrol includes Spam reports, Monitoring reports, Anti-virus reports, Traffic reports, Rule reports and Attachment reports.

17.4.1 Spam Reports

Spam reports can be used to gain insight into the effectiveness of spam blocking and the amount of spam received.

Report	Type	Description
Top spam senders	List	Top 10, 25, 50 or 100 spam senders.
Top spam receivers	List	Top 10, 25, 50 or 100 spam receivers.
Top spam domains	List	Top 10, 25, 50 or 100 spam sending domains.

Top spam IP addresses	List	Top 10, 25, 50 or 100 spam sending IP addresses.
Spam received	Graph	Number of spam messages received.
Spam/legitimate email	Pie	Spam/legitimate email overview.
Address harvest attempts	Graph	Number of address harvest attempts.
Recipients rejected	Graph	Number of recipients rejected.
Emails from Senders on the Allow List	Graph	Number of emails added to the allow list.
Emails from Senders on the Block List	Graph	Number of emails added to the block list.
Sender Policy Framework	List	SPF checking results.
DNSBL lists (SMTP)	Graph	Number of emails listed on DNSBL lists, checked at SMTP level.
DNSBL lists (headers)	Graph	Number of emails listed on DNSBL lists, checked in headers.
SURBL lists	List	SURBL checking results.
Spam characteristics	List	Spam characteristics filtering results.
Challenge/response sent by day	Graph	Number of challenge/response requests sent by day.
Challenge/response sent by hour	Graph	Number of challenge/response requests sent by hour.
Challenge/response replies	List	Details of challenge/response replies
Anti-spam actions taken	List	Number of times each action was taken.

17.4.2 Monitoring Reports

Monitoring reports show how many messages have been blocked and released.

Report	Type	Description
Messages blocked by hour	Graph	Number of messages blocked by hour.
Messages blocked by day	Graph	Number of messages blocked by day.
Messages released by hour	Graph	Number of messages released by hour.
Messages released by day	Graph	Number of messages released by day.

17.4.3 Anti-Virus Reports

Anti-virus reports show how many viruses have been found and where they are coming from.

Report	Type	Description
Anti virus statistics	List	Anti virus statistics
Top virus names	List	Top 10, 25, 50,100 viruses.

17.4.4 Traffic reports

Traffic reports provide insight into how many messages are being sent and received on the network as well as the size of the messages.

Report	Type	Description
Traffic by local domain	List	Number and size of internal/external messages sent and received per local domain.
Traffic by local users	List	Number and size of internal/external messages sent and received per user.

17.4.5 Policy Reports

Policy reports show how often policies have triggered and how many messages are released out of quarantine.

Report	Type	Description
Policies triggered by local domain	List	Number of times policies have triggered per local domain.
Policies triggered by local users	List	Number of times policies have triggered per user.

17.4.6 Attachment Reports

Attachment reports are used to gain insight into the number, types and sizes of attachments that are being sent on the network.

Report	Type	Description
Attachments by local domain	List	Type and size of attachments per local domain.
Attachments by local users	List	Type and size of attachments per user.
Attachment types by local domain	List	Attachment types per local domain.
Attachment types by local users	List	Attachment types per user.

Chapter 18

Settings

Policy Patrol includes several options that can be configured from the settings node, including languages, schedules, HTML stationery and users. This chapter describes how these features can be configured. Filters and Templates are discussed in chapters 12 and 13 respectively.

18.1 Languages

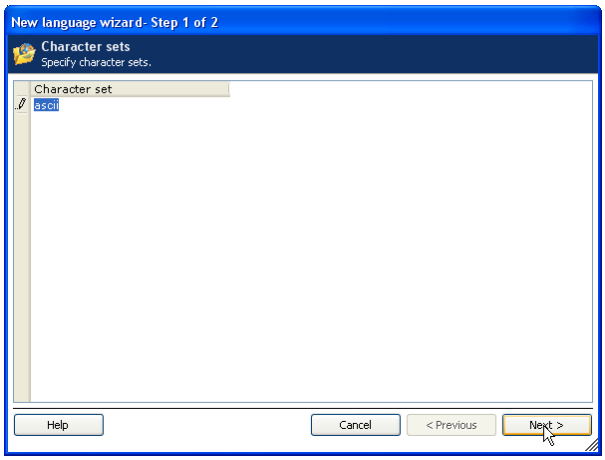
In **Settings** > **Languages**, the different language code pages can be configured. Policy Patrol already includes a number of languages. However, if you need to add more or make changes to existing languages, you can do so by following the next steps:

1. Click **New**. The new Language wizard will start up.

2. Click **Next** in the Welcome screen.



3. Enter the character sets for the language. The character set of a message can be found in the message header and is displayed as follows: charset = "xxx", e.g. charset="us-ascii". When you are done, click **Next**.



4. Enter the Language name and description and click **Finish**.

18.2 Attachment Maps

Policy Patrol includes more than 100 attachment maps which are used to check whether files are spoofed. Normally you would not need to enter any further attachment maps, but if you wish to do so you can do this as follows:

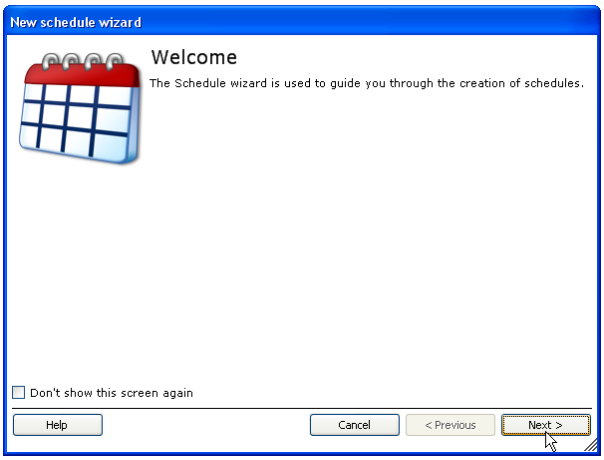
1. Go to **Settings** > **Attachment Maps**. Click on **New**. Click **Next** in the Welcome screen.

2. Enter the file extension, description and attachment map. Click **Finish**.

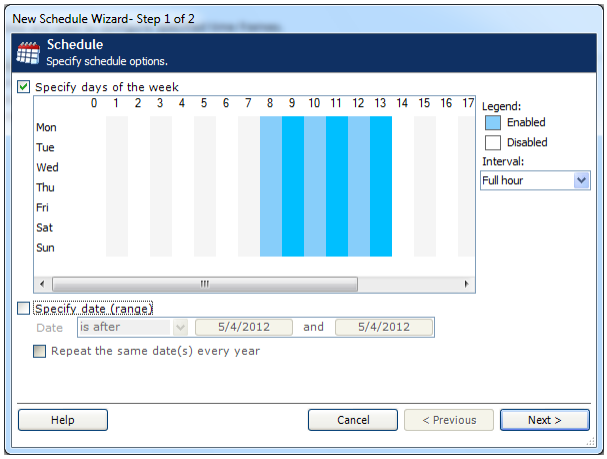
18.3 Schedules

This node displays the existing schedules that can be selected when scheduling a policy. To create a new schedule:

1. Go to **Settings** > **Schedules**. Click **New**. The Schedule wizard will appear. Click **Next** in the Welcome screen.



2. Specify the schedule settings. If you wish to include certain days and times of the week, select the option **Specify days of the week** and select the days and hours the schedule must include. The selected hours will be displayed in blue. If you wish to specify half hours and quarter hours, select the **Half hour** or **Quarter hour** option from the Interval drop-down box. Note that the number that you select is when the schedule begins, e.g. if you select full hour and specify 8 until 13 (see screen below), the schedule will run from 8.00 until 14.00.



   To apply a schedule on certain dates, select **Specify date (range)**. Specify whether the schedule must apply when the date **equals**, **is after**, **is before**, **is between** or **is not between** specific date(s). Enter the appropriate date(s). If you select after or before, the policy will not run on the actual date selected, but after or before it. For instance, if you select that a schedule must apply after January 1st, it will start on January 2nd. If you select before January 1st, the schedule will apply on any date before, but not including January 1st. If you select between or not between, the schedule will apply/not apply between and including the dates selected. For example, if you configure a schedule and select **is not between** January 1st and January 3rd, it will not run on January 1st, January 2nd and January 3rd. If you create a schedule and select **is between** January 1st and January 3rd, it will apply on January 1st, January 2nd and January 3rd. If you wish the schedule to apply on the same dates each year, select the option **Repeat the same date(s) every year**.

3. Enter a name and description for the Schedule. Click **Finish**.

To edit an existing schedule, select the schedule in the list and click **Edit**. Make the appropriate changes and click **OK**. To rename a schedule, right click the schedule and click **Rename**. Make the changes and press [Enter]. To remove a schedule, right-click the schedule and select **Remove**. Remember that you cannot delete any schedules that are being used in a policy.

To copy an existing schedule, right-click the schedule and select **Duplicate**. The schedule will now be duplicated. The name will be displayed as follows: Copy of <original schedule name>.

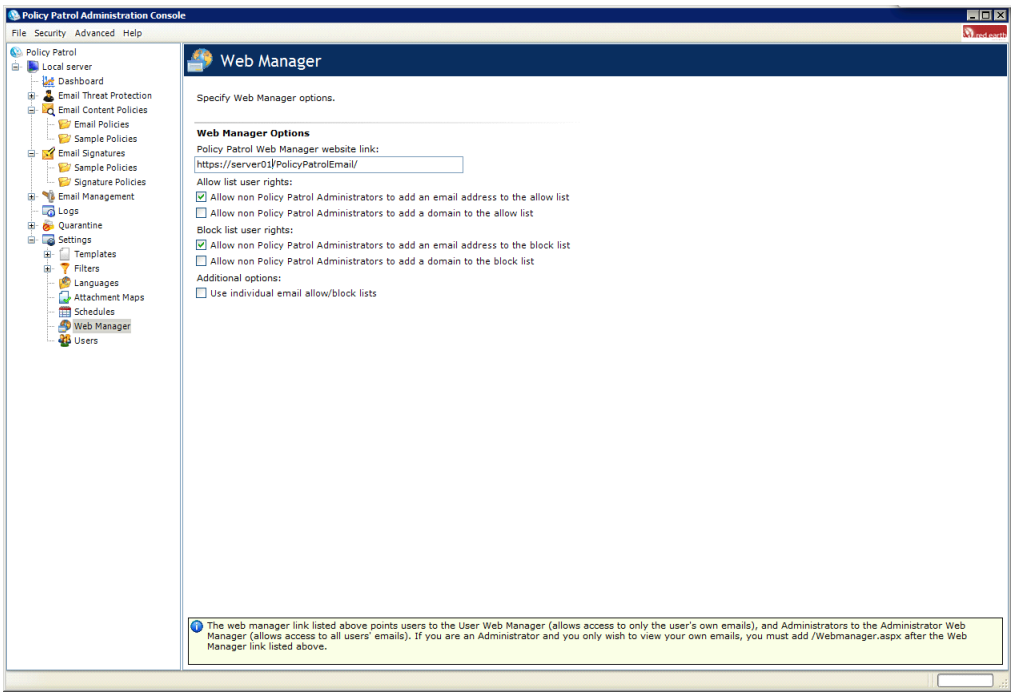
18.4 Web Manager Options

Here you can edit the link for the web manager and set user permissions for the web manager.

By default the link is http://<servername>/policypatrolemail/, where servername is the name of the Policy Patrol machine, for instance http://server01/policypatrolemail.

Instead of <servername> you can also enter the IP address of the Policy Patrol, however in that case the user will be prompted for user credentials. When the <servername> is used in the URL, Windows Integrated Authentication will be used and the user will not be asked to enter their credentials.

The web manager link points users to the User Web Manager (allows access to only the user's own emails), and Administrators to the Administrator Web Manager (allows access to all users' emails). If you are an Administrator and you only wish to view your own emails, you must add /webmanager.aspx after the web manager link as follows: http://<servername>/policypatrolemail/webmanager.aspx. Only users with Administrator rights are allowed access to the Administrator Web Manager.



18.4.1 Allow List User Rights

The following Allow list user rights can be configured for the Web Manager:

☑ Allow non Policy Patrol Administrators to add an email address to the allow list

If this option is not checked:

(1) The **Deliver & add to allow list** button in Web Manager is not displayed for non-Policy Patrol Administrators.

(2) If a non-Policy Patrol Administrator goes to the white list page in the Web Manager, enters an email address and clicks 'Submit' they will see the following error message: 'You don't have rights to perform this action'.

(3) If a non-Policy Patrol Administrator clicks on 'Deliver & add to allow list' in the Quarantine report, the user will see the following error message: 'You don't have rights to perform this action'.

☑ Allow non Policy Patrol Administrators to add a domain to the white list

If this option is not checked:

(1) If a non-Policy Patrol Administrator goes to the allow list page in the Web Manager, enters a domain and clicks 'Submit' they will see the following error message: 'You don't have rights to perform this action'

* If both allow list user rights are not checked and a non-Policy Patrol Administrator goes to the Allow list page in the Web Manager, they will see this error message: 'You are not authorized to view this web page'. Note that it is also possible to remove the 'add to allow list' and 'add to block list' links in the Web Manager (see knowledge base for instructions), however if you hide the links in the User Web Manager the links will be hidden in the Administrator Web Manager too.

18.4.2 Block List User Rights

The following block list user rights can be configured for the Web Manager:

☑ Allow non Policy Patrol Administrators to add an email address to the block list

If this option is not checked:

(1) **Delete & add to block list** button in Web Manager is not displayed for non-Policy Patrol Administrators.

(2) If a non-Policy Patrol Administrator goes to the block list page in the Web Manager, enters an email address and clicks 'Submit' they will see the following error message: 'You don't have rights to perform this action'.

(3) If a non-Policy Patrol Administrator clicks on 'Delete & add to block list' in the Quarantine report, the user will see the following error message: 'You don't have rights to perform this action'.

☑ Allow non Policy Patrol Administrators to add a domain to the block list

If this option is not checked:

(1) If a non-Policy Patrol Administrator goes to the block list page in the Web Manager, enters a domain and clicks 'Submit' they will see the following error message: 'You don't have rights to perform this action'.

* If both block list user rights above are not checked and a non-Policy Patrol Administrator goes to the Block list page in the Web Manager, they will see this error message: 'You are not authorized to view this web page. Note that it is also possible to remove the allow list and block list links in the Web Manager (see knowledge base for

instructions), however if you hide the links in the User Web Manager the links will be hidden in the Administrator Web Manager too.

18.4.3 Additional Options

☑ Use individual email allow/block lists

If this option is enabled and users add an email address or domain to the Allow or Block List from the web manager, the entry will only be applied to their own emails. For instance if user JamesC adds the email address johndoe@gmail.com to the allow list, mail from this email address will only be considered on the allow list when addressed to jamesc@company.com. If the email from johndoe@gmail.com is addressed to another user in the company (i.e. other than jamesc@company.com) the sender will not be considered as listed on the allow list. In the Email Allow list (under Anti-spam > Allow > Email Allow List), the entry johndoe@gmail.com will have `JamesC` listed in the **Scope** column. This means that this allow list entry will only apply to emails sent to JamesC. Entries in the allow and block lists that apply to all users have `[Global]` listed as the scope. Note that when an Administrator adds an email address to the Allow or Block List, it will always have `[Global]` as the scope.

18.5 Users

This node includes a list of all your licensed users. For each user the name, type and email address is listed.

To delete a licensed user, select the user and press the **Remove** button. If you move users, groups or objects in the Active Directory their location will automatically updated in Policy Patrol. However, in case you would like to initiate this process manually, this can be done by clicking on the **Verify users/groups** button. If a user can no longer be located in the Active Directory, a dialog will pop up asking whether you wish to remove this user from licensing. For more information on how to license users, please consult the chapter 'Importing users'.

Chapter 19

Dashboard

Policy Patrol 10 includes a new dashboard to give you an overview of emails processed, and the different actions that have been taken on emails for the selected time period.

19.1 Email Threat Protection

In the Email Threat Protection section, you can get an overview of the number of emails processed, and blocked threats such as spam, phishing, malware and files sanitized.

19.2 Email Content Policies

This section lists the different configured policies and how often they have been applied in the selected time period.

19.3 Email Management

This section provides insight into the Email Management tools and how often they have triggered.

19.4 Email Signatures

This section includes a list of all the active email signatures and how often they have been applied in the selected time period.

19.5 Quarantine Folders

In Quarantine folders, you can see how many emails where deleted, quarantined and released from the quarantine in the selected time period.

Chapter 20

Server Administration

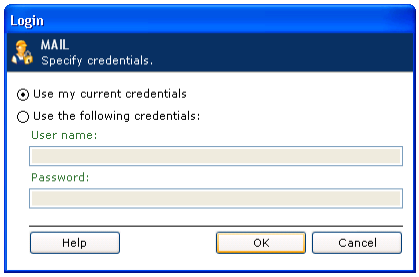
Policy Patrol includes some server options & settings that can be configured from the Policy Patrol server node(s), including user security, system configuration, system parameters, and automatic updates.

20.1 User Security

In User security you can give selected users access to the Policy Patrol Administration console and grant them certain permissions within the Administrations console. Policy Patrol user security is implemented at three levels; user access rights, component rights and folder rights.

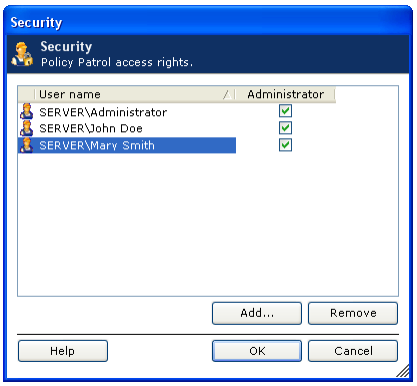
20.1.1 User Access Rights

When a user connects to a Policy Patrol server, they will be asked for log on credentials. The user can log on with the current credentials or specify another user name and password. Policy Patrol will then check these credentials to see if the user is permitted to access the Policy Patrol Administration console.



By default only the members of the Administrator group are allowed to connect to Policy Patrol installations. To define which users have access rights, follow the next steps:

1. Select **<server name>**, expand **Security** and click on **User security**.

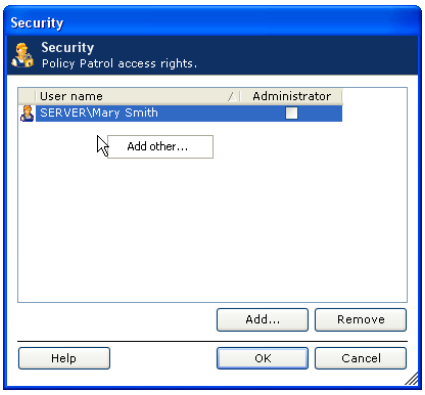


2. To add a user with access rights to Policy Patrol, click on **Add**. Select the users you wish to add and click **OK**. To remove a user from the list, select the user and click **Remove**.

3. To give the user Administrator rights, select the user and tick the check box **Administrator rights**. The user icon will now include a small lock to indicate that it has administrative rights. Policy Patrol Administrators have full access to all components and folders and cannot be denied any permissions. You must make at least one user an Administrator so that this user will always be able to access all options in Policy Patrol.

Note

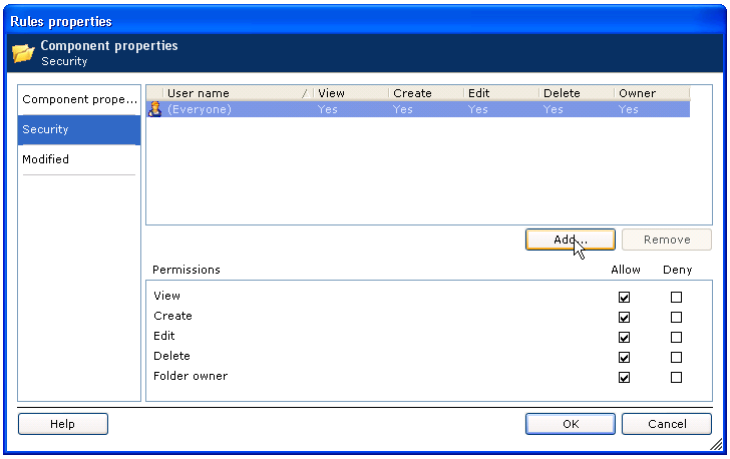
If you wish to grant a user from another domain access rights, you can right-click in the Security list and select **Add other**. This will allow you to specify a user by entering the user name in DOMAIN\Username format.



20.1.2 Component Rights

Now that you have set the access rights to the Administration console, you can specify which Policy Patrol components (i.e. tree nodes) each user has access to. By default, each user has access to all components. To change the access rights for a certain component, follow the next steps:

1. Right-click the component (for instance **Email Content Policies**) and choose **Component properties...**



2. Go to the **Security** tab. By default the (Everyone) group has full access to the component. To change permissions, select the group and change the Allow/Deny permissions. The following rights can be applied:

Right	Description
View	View items
Create	Create new items
Edit	Edit existing items
Delete	Delete items
Folder owner	Change folder permissions

If you only wish certain users to have rights to the component, click on **Add** and select the user(s) with the permissions. Select **Allow** or **Deny** for the relevant rights. Then select **Everyone** and click **Deny** for all rights.

If you wish all users to have access to the component apart from a couple of exceptions, click on **Add** and select the users to be denied access. Select the user(s) and tick the **Deny** check boxes.

A Folder owner has the right to change the component permissions for the component. Therefore, if you wish to deny permissions for a user, you must also select **Deny** for the **Folder owner** right.

Remember that each component needs to have at least one Folder owner and that Administrators cannot be denied any permissions.

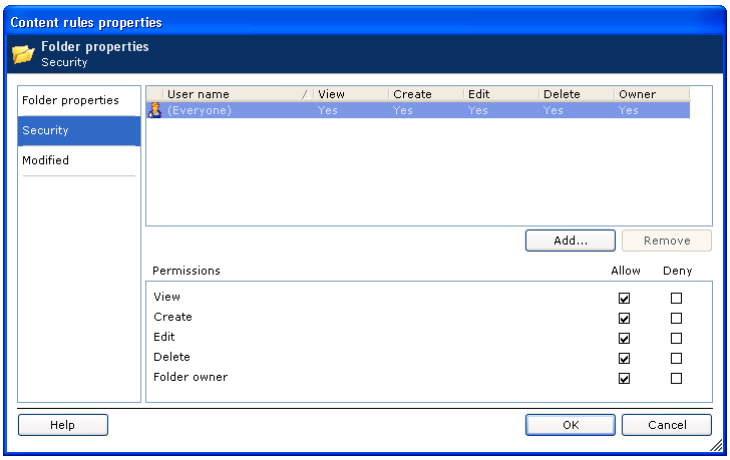
When you have finished editing permissions, click **OK**.

20.1.3 Folder Rights

Policy Patrol makes use of folders for structuring purposes and to provide the possibility of controlling user access and rights to different folders. Policy Patrol includes a number of sample folders but you can also create your own folders.

To create a new folder, right-click the component and choose **New folder**… If you wish to create a subfolder, you must right-click on the parent folder and choose the option **New folder...** By default all users are given full rights to all folders. To change the permissions for a folder, follow the next steps:

1. Right-click the folder and select **Folder properties...**.



2. Go to the **Security** tab. By default the (Everyone) group has full access to the folder. To change permissions, select the group and change the Allow/Deny permissions. The following rights can be applied:

Right	Description
View	View items
Create	Create new items
Edit	Edit existing items
Delete	Delete items
Folder owner	Change folder permissions

If you only wish certain users to have rights to the folder, click on **Add** and select the user(s) with the permissions. Select **Allow** or **Deny** for the relevant rights. Then select **Everyone** and click **Deny** for all rights.

If you wish all users to have access to the folder apart from a couple of exceptions, click on **Add** and select the users to be denied access. Select the user(s) and tick the **Deny** check boxes.

A Folder owner has the right to change the folder permissions for the folder. Therefore, if you wish to deny permissions for a user, you must also select **Deny** for the **Folder owner** right.

Remember that each folder needs to have at least one Folder owner and that Administrators cannot be denied any permissions.

20.1.4 Inheritance of Folder Rights

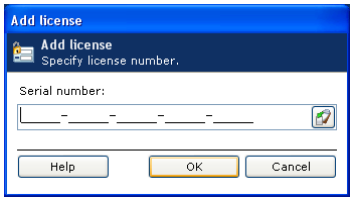
If you create a subfolder, the subfolder will inherit the permissions of the top folder. If you edit the rights for a folder that contains subfolders, the same changes will be applied to the subfolders.

Note

Policy Patrol Administrators have full rights to all components and folders and cannot be denied any permissions. If you wish to block access for a user with Administrator rights, you must first remove the Administrator rights for the user in **<server name>** > **Security** > **User security**..

20.2 Licensing

To enter your serial number in Policy Patrol, select **Security** > **Licenses** from the menu. 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.



Note

If you are entering a serial number for a different Policy Patrol edition than you currently have enabled (for instance if you were evaluating Policy Patrol Enterprise and have purchased Policy Patrol Disclaimers), a message will pop up saying that the license is for a different Policy Patrol edition and that any existing serial numbers will be removed. Click **Yes** to continue. Click **OK** to close the Licenses dialog. Another message will appear warning you that Policy Patrol will need to reconnect to the server. Click **OK**.

20.3 System Configuration

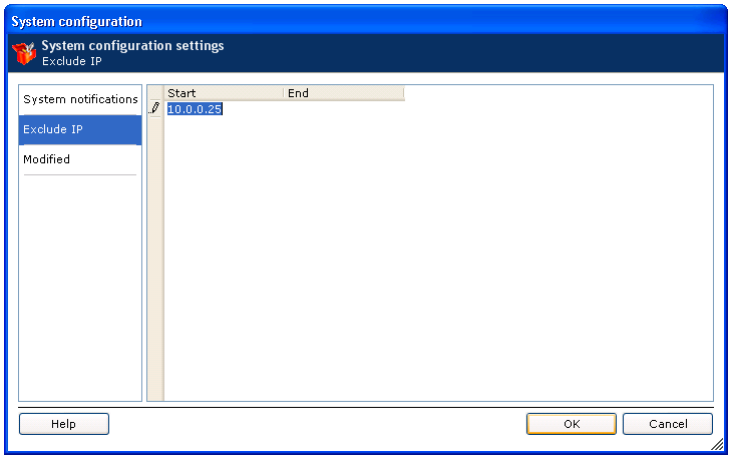
System configuration options are found in **<server name>** > **Advanced** > **System configuration**. The following tabs are available:

20.3.1 System Notifications

In this tab you can specify the options for system notifications. In the From: field, enter the sender of the email. 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 sending notification messages.

20.3.2 Exclude IP

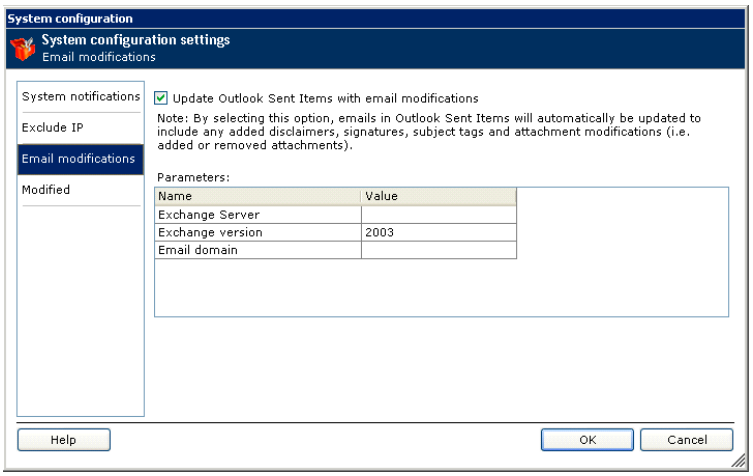
If you do not want Policy Patrol to process messages sent from a certain IP address, you can enter the IP address(es) in this Exclude IP list. To enter a single IP address, enter the IP address in **Start**. To enter an IP range, enter an IP address in **Start** and **End**.



20.3.3 Email Modifications

Policy Patrol can automatically update the emails in Outlook Sent Items to include any email modifications that Policy Patrol might have applied to the email, including disclaimers, signatures, added/removed attachments and subject modifications. The advantages of updating Outlook Sent Items are as follows:

- Obtain proof that your disclaimer was added
- View the formatting of your signature
- Your email archive will contain the actual email that was sent or received



To update Outlook Sent Items, check the option **Update Outlook Sent Items with email modifications**.

Note that for Sent Items in Outlook to be updated, Policy Patrol must be installed on an Exchange 2003, 2007, 2010 or 2013 machine. Under Parameters a number of options are listed. You do not need to change these settings unless the below scenarios apply or you are directed to enter any of these values by Policy Patrol technical support.

20.3.3.1 If You Have Multiple Exchange 2007/2010/2013 Servers

If you have more than one Exchange 2007/2010/2013 Server, please follow the instructions below:

Note

If you only have one Exchange Server or if you have Exchange 2003 you do not need to follow these instructions.

1. In 'Exchange version' your Exchange version should be entered (2007, 2010 or 2013).

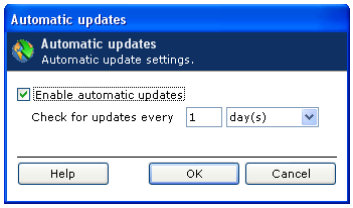
2. In 'Exchange Server (CAS)' the name of your Exchange Client Access Server should be listed (even if this is the same machine as Policy Patrol is installed on). If you have multiple Exchange Servers, you need to enter the name of your Client Access Server (CAS). If you have multiple Client Access Servers (load balancing) you need to enter the virtual IP address that is used for load balancing. The Policy Patrol Sent Items updates will then also be load balanced.

20.4 System Parameters

System parameters are found in **<server name>** > **Advanced** > **System Parameters**. Policy Patrol system parameters are similar to registry keys and must not be changed unless you are asked to do so by Policy Patrol technical support staff.

20.5 Automatic Update Settings

Policy Patrol can notify you when there are new Policy Patrol updates. Tick the option **Enable automatic updates** if you wish to receive notifications when updates become available. The notifications will be sent to the email addresses specified in **server name>** > **Advanced** > **System configuration > System notifications**.



20.6 Import Policy Patrol Configuration

To import a complete Policy Patrol configuration (this will overwrite the current configuration), select the option **Import Policy Patrol Configuration**. Policy Patrol will temporarily be stopped whilst importing the configuration. Select the file to import from and click **Open**.

20.7 Export Policy Patrol Configuration

To export the complete Policy Patrol configuration for use on another machine or for back up purposes, select the option **Export Policy Patrol Configuration**. Policy Patrol will temporarily be stopped whilst exporting the configuration. Enter a file name (that ends in .ppe) and click **Save**. To import the configuration on another machine, select the option **Import Policy Patrol Configuration**.

20.8 Disabling Policy Patrol

If you wish to disable Policy Patrol, i.e. you do not wish Policy Patrol to intercept and process any messages, follow the steps described below depending on the version you have.

20.8.1 To Disable Policy Patrol 32-bit

Run the following commands from a command prompt in the folder where smtpreg2.vbs is located (by default C:\Program Files\Red Earth Software\Policy Patrol Email:

cscript smtpreg2.vbs /disable 1 oninboundcommand PP8_MailFrom
cscript smtpreg2.vbs /disable 1 oninboundcommand PP8_RcptTo
cscript smtpreg2.vbs /disable 1 onpostcategorize PP8_PostCategorize

20.8.2 To Disable Policy Patrol 64-bit

Run the following commands in Exchange Management Shell (Note that after modifying registrations a restart of the 'Microsoft Exchange Transport' service is required):

Disable-TransportAgent:

Name: Policy Patrol Email Edge

Disable-TransportAgent:
Name: Policy Patrol Email Hub

20.9 Enabling Policy Patrol

If you wish to enable Policy Patrol again after it has been disabled, follow the steps described below depending on the version you have. Policy Patrol will then start intercepting and processing messages again.

20.9.1 To Enable Policy Patrol 32-bit

Run the following commands from a command prompt in the folder where smtpreg2.vbs is located (by default C:\Program Files\Red Earth Software\Policy Patrol Email:

cscript smtpreg2.vbs /enable 1 oninboundcommand PP8_MailFrom
cscript smtpreg2.vbs /enable 1 oninboundcommand PP8_RcptTo
cscript smtpreg2.vbs /enable 1 onpostcategorize PP8_PostCategorize

20.9.2 To Enable Policy Patrol 64-bit

Run the following commands in Exchange Management Shell (Note that after modifying registrations a restart of the 'Microsoft Exchange Transport' service is required):

Enable-TransportAgent:
Name: Policy Patrol Email Edge

Enable-TransportAgent:
Name: Policy Patrol Email Hub

Chapter 21

Troubleshooting

This chapter describes how to troubleshoot Policy Patrol. If you have a problem you can consult the Policy Patrol online knowledge base, or request support from Red Earth Software.

21.1 Knowledge Base

If you have a question or problem with Policy Patrol you can consult our extensive online knowledge base at https://support.redearthsoftware.com/forums. Some of the questions and answers are listed below. If you do not find your answer, please send an email to support@redearthsoftware.com.

21.1.1 No Disclaimers are Being Added

If no disclaimers are being added, please check the following points:

1. Make sure that you have entered text in both the **HTML** and **RTF/Plain** tab of the disclaimer template. If you don't enter any text in the HTML tab, no disclaimers will be added to HTML mails. If you don't enter any text in the RTF/Plain tab, no disclaimers will be added to plain text and rich text mails.

2. Make sure that the policy that adds disclaimers is enabled. To check this, go to **Email Signatures** > **<folder name>**. If the rule has an icon with a red stop sign in it, it is disabled. Right-click and select **Enable**.

3. Go to **Logs** > **Message History** and locate the email in the list (if the Message history is empty, please consult the KB article 'Policy Patrol is not processing any messages'). In the bottom pane, click on **Policy report**. Did the disclaimer policy trigger? If it did trigger but no disclaimer was added, the reason is probably that there is no text in the disclaimer template (see point 1) or the option **Add disclaimer/signature only once** is checked and the message already includes a disclaimer. If the disclaimer policy did not trigger, click on the sign to expand further information on why the policy did not trigger and check the appropriate settings in your disclaimer policy: Policy users, Policy direction, Policy exceptions, Policy schedule.

4. If you have checked the above and disclaimers are still not being added, please send us your support files by going to **Help** > **Send support files**. Red Earth Software technical support will then be able to look into the problem.

21.1.2 My Sent Items in Outlook are not Being Updated

If your Outlook Sent Items are not being updated with email disclaimers, signatures and other modifications, please check the following:

1. Go to **Local server** > **Advanced** > **System Configuration**. Click on the **Email Modifications** tab. Is the option **Update Outlook sent items with email modifications** selected? If not, please select it. Note that this option is only available when Policy Patrol is installed on the Exchange Server.

2. Is Policy Patrol installed on Exchange Server 2003/2007/2010? Policy Patrol must be installed on Exchange 2003/2007/2010 in order to update the Sent Items.

3. Do you have multiple 2007/2010/2013 Exchange Servers? If so, follow the instructions in 19.3.3.1.

4. Is the **Policy Patrol Email Simple Information Store Access Service** started? If not, start it.

5. Make sure that the PolicyPatrolIS account is not a Domain Administrator account.

6. Are your users using Outlook in cached mode? If so, send an email to support@redearthsoftware.com and we will send you instructions.

If you have checked the above and your Sent Items are still not being updated, please contact support@redearthsoftware.com.

21.1.3 User Merge 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. Click on the **Preview** icon in the toolbar (the looking glass) and check whether the fields are being replaced correctly.

- ☑ 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 a Lotus Domino field, verify that information is entered in the Lotus Domino mailbox properties for the user.

- ☑ 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.

21.1.4 I Cannot Enter Licenses or Browse to Files or Folders

Licensing options and file browsing are not available when remotely configuring Policy Patrol through Policy Patrol Remote Administration. Instead of browsing, the path to the folder or file must be entered. Serial numbers must be entered on the Policy Patrol server installation.

21.1.5 How Can I Copy the Configuration to Another Machine?

You can export your Policy Patrol configuration and import it into another installation. To do so, in the Policy Patrol Administration console select **File** from the menu and select **Export Configuration**. Policy Patrol will be temporarily stopped whilst exporting the configuration to a .ppe file. In the new Policy Patrol installation, go to **File** and select **Import Configuration**. Select the .ppe file. Policy Patrol will be temporarily stopped whilst importing the new configuration. Note that any existing configuration will be overwritten.

21.2 Send Support Files

If you have checked the manual and knowledge base and you are still having problems, please forward your support files to Red Earth Software technical support by selecting **Help** > **Support Files**. Enter your contact details and provide a detailed problem description. Leave the checkboxes **Include Policy Patrol configuration files** and **Include Policy Patrol log files** enabled unless you have been asked to uncheck one of them. Select **Save support files on the hard drive**, and upload them at http://www.policypatrol.com/support/support-files/.

21.3 Contacting Red Earth Software

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

Red Earth Software, Inc.
4845 Pearl East Circle, Ste. 101
Boulder, CO 80301
United States
Toll-free: 1 (800) 921-8215
Phone: (720) 377 3728
Fax: (720) 554 7950
Sales: sales@redearthsoftware.com
Support: support@redearthsoftware.com

Red Earth Software (UK) Ltd
20 Market Place
Kingston-upon-Thames
Surrey KT1 1JP
United Kingdom
Tel: +44-(0)20-8328 9830
Fax: +44-(0)20-8711 5771
Sales: sales@redearthsoftware.co.uk
Support: support@redearthsoftware.co.uk

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

Index

A

Actions · 103, 125
Active Directory · 167, 170, 171
Add attachment · 107
Add business card · 106
Add From: domain/email address to filter · 111
Add To: domain/email address to filter · 111
Administrator address(es) · 239
Anti-virus · 137, 224, 225
Archive message · 104, 119, 136, 149
Attachment contains word/phrase · 101, 218
Attachment exists · 99, 124, 216
Attachment name · 114, 136, 141, 142
Attachment Name Filter · 142
Attachment size · 99, 217
Avatar · 160

B

Bayesian filtering · 66
Binary text file · 100, 218
Body · 90, 98, 119, 123, 209, 216, 224
Bold · 149

C

Case sensitive · 45, 46, 50, 51, 138, 141, 142
Challenge/response · 35, 71, 72, 73, 170, 176, 225
Change priority/importance · 107
CLSID extension · 100, 217
Clustering · 7
Conditions · 90, 119, 208, 219
Connector · 23, 26
Convert to plain text · 106
Counter fields · 169

D

Date/Time fields · 169
Default value · 171
Delay message · 137
Delivery receipt request · 93, 106, 211
Delivery Status Notification · 93, 108, 120, 211
Details · 181
Digitally signed · 90, 120, 209
Disclaimer · 114, 126, 127, 130, 135, 136, 150, 151, 152, 156
DNS white lists · 47
Domain controller · 23
Domain/Email address filter · 143

E

Encrypted · 90, 120, 209
Exceptions · 89, 103, 118, 124, 136, 219
Exchange 2000 · 6, 23
Exchange 2003 · 6, 105, 212
Exchange 2007 · 6, 12, 18, 23, 106, 109, 111, 149
Exchange 2010 · 6, 23
Exchange 2013 · 6
Export · 46, 51, 141, 142, 143, 149, 154, 158
External messages · 91, 168, 169, 209

F

False positives · 54
FAQs · 243
Field prefix · 170
Font color · 149
Font size · 149
Font type · 149
Frequently asked questions · 243

G

Gravatar · 160, 161

H

HTML format · 108
HTML source · 98, 123, 216
HTML stationery · 2, 227

I

Import · 46, 51, 141, 142, 143, 149, 154, 158
Inline attachments · 99, 124, 217
Insert Field · 146, 148, 152, 157
Insert image · 149, 154, 158
Installation · 10
Internal messages · 106, 131, 169, 239
Italics · 149

J

junk mail folder · 74

K

Knowledge Base · 243

L

Lotus Notes · 7
Lotus Notes/Domino · 5, 7

M

Match all of the conditions · 90, 119, 209
Match any of the conditions · 90, 119, 209
meCard · 162, 163
Message date · 92, 210
Message fields · 168
Message format · 91, 209
Message priority · 91, 120, 210
Message report · 179
Message sensitivity · 91, 120, 210
Message size · 91, 210
Microsoft .NET Framework · 5, 18
Monitoring · 179
MSDE · 223
Multiple extensions · 100, 217

N

Network message · 111
Non-inline attachments · 99, 124, 217
Notification message · 36, 93, 108, 110, 114, 120, 146, 147, 149, 169, 211
Number of attachments · 102, 219
Number of recipients · 96, 214

O

On hold · 179
Ordering · 114, 131, 136
Outlook Sent Items · 239

P

Permissions · 3, 177, 178, 235, 236, 237, 238
Plain text · 2, 91, 106, 108, 147, 151, 152, 169, 180, 209
POP3 clients · 7
POP3 downloader · 204
Primary actions · 103, 125
Process following rule(s) · 115, 132

Q

QR Code · 162, 163
Quarantine message · 137
Quarantine remarks · 168

R

Read receipt request · 93, 106, 211
Regular Expression · 45, 46, 50, 51, 139, 140, 141
Reject message · 183
Remote administration · 18
Remove attachment · 107
Rename · 116, 133, 145, 166
Replace words/phrases in subject · 105, 106, 130
RTF/plain text · 127, 151

S

Schedules · 228
Scope · 42, 48, 232
Secondary actions · 103, 104, 114, 125, 131, 136
Send blind copy · 109, 131
Sender field contains domain or email address · 95, 122, 213
Spamhaus Block List (SBL) · 47, 55
Spoofed attachment · 100, 217
SQL Server Express · 208, 223
Subject · 90, 97, 98, 119, 123, 136, 168, 209, 215, 216
SURBL Lists · 57
System parameters · 240
System requirements · 5

T

Tag · 98, 104, 114, 123, 136, 150, 216
Tag template · 149
Templates · 146, 150, 166
Thumbnail picture · 160
Tracking numbers · 169

U

Underline · 149
User fields · 167, 171
Users · 7, 23, 26, 89, 104, 118, 136

V

VCard · 106
Verify attachment extension · 100, 217
Virus · 100, 168, 217, 218

W

Web manager · 193
Whole or part of word(s) are matched · 45, 51, 140, 141
Whole word(s) are matched · 45, 51, 140, 141

Word score · 45, 46, 50, 51, 140, 141
Word score threshold · 45
Word/Phrase filter · 138

X

X-Header · 97, 105, 215