Manual

POLICY PATROL EMAIL

DISCLAIMERS & SIGNATURES



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 Signatures 33

6 How to Order Policies 52

7 Creating Filters 55

8 Creating Templates 63

9 Logs 90

10 Email Management 95

11 Settings 100

12 Dashboard 102

13 Server Administration 103

14 Troubleshooting 112

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 Signatures 33

5.1 Configuring a Signature Policy 33

5.1.1 Step 1. Policy Users 34

5.1.2 Step 2. Policy Direction 35

5.1.3 Step 3. Policy Conditions 35

5.1.4 Step 4. Policy Exceptions 40

5.1.5 Step 5. Policy Actions 41

5.1.5.1 Primary Actions 41

5.1.5.2 Secondary Actions 41

5.1.5.3 Ordering of Secondary Actions 47

5.1.6 Step 6. Policy Scheduling 48

5.1.7 Step 7. Policy Name 48

5.2 Editing Existing Policies 49

5.3 Copying Policies 49

5.4 Moving Policies 49

5.5 Signature Position Maps 50

5.6 Viewing Signatures in Outlook Sent Items 50

6 How to Order Policies 52

6.1 Ordering Policies 52

6.1.1 Processing Speed 52

6.1.2 Ordering Result 53

6.1.3 Process Next Policies 54

7 Creating Filters 55

7.1 Creating a Word/Phrase Filter 55

7.2 Creating an Attachment Filter 58

7.3 Creating an Email/Domain Filter 60

7.3.1 Active Directory Users in Email Filter 61

7.4 Editing Filters 61
7.5 Copying Filters 62
7.6 Moving Filters 62
7.7 Content Checking Attachments 62

8 Creating Templates 63

8.1 Creating an Email Notification Template 63
8.2 Creating a Tag Template 66
8.3 Creating a Disclaimer/Signature Template 67
8.3.1 Creating a Standard Disclaimer/Signature Template 67
8.3.2 Creating an HTML Stationery Disclaimer Template 72
8.4 Inserting an Avatar in the Email Signature 77
8.5 Inserting a QR Code in the Email Signature 79
8.6 Inserting Images or URLs from Active Directory 82
8.6.1 Inserting an AD Image into the Email Signature 82
8.6.2 Inserting a Personalized URL into the Email Signature 82
8.7 Editing Templates 83
8.8 Copying Templates 83
8.9 Moving Templates 83
8.10 Fields 83
8.10.1 User Fields 84
8.10.2 Message Fields 85
8.10.3 Date/Time Fields 86
8.10.4 Other Fields 86
8.11 Inserting AD Fields Depending on User's AD Information 87
8.11.1.1 Using a Prefix only if the Field Exists 87
8.11.1.2 Avoiding an Empty Line if a Field Does Not Exist 87
8.11.1.3 Specifying a Default Value if a Field Does not Exist 88
8.12 Configuring Additional Directory Fields 88

9 Logs 90

9.1 History 90
9.1.1 Message Report 91
9.1.2 Email Threats Report 91
9.1.3 Email Content Policies Report 92
9.1.4 Email Signatures Report 92
9.1.5 Email Management Report 92
9.1.6 Viewing Details 93
9.2 Event History 93
9.3 Audit Logs 94

10 Email Management 95

10.1 Auto Replies 95
10.2 POP3 Downloader 97

11 Settings 100

11.1 Schedules 100
11.2 Users 101

12 Dashboard 102

12.1 Email Threat Protection 102
12.2 Email Content Policies 102
12.3 Email Management 102
12.4 Email Signatures 102
12.5 Quarantine Folders 102

13 Server Administration 103

13.1 User Security 103
13.1.1 User Access Rights 103
13.1.2 Component Rights 104
13.1.3 Folder Rights 106
13.1.4 Inheritance of Folder Rights 107
13.2 Licensing 107
13.3 System Configuration 107
13.3.1 System Notifications 108
13.3.2 Exclude IP 108
13.3.3 Email Modifications 108
13.3.3.1 If You Have Multiple Exchange 2007/2010/2013 Servers 109
13.4 System Parameters 109
13.5 Automatic Update Settings 110
13.6 Import Policy Patrol Configuration 110
13.7 Export Policy Patrol Configuration 110
13.8 Disabling Policy Patrol 110
13.8.1 To Disable Policy Patrol 32-bit 110
13.8.2 To Disable Policy Patrol 64-bit 110
13.9 Enabling Policy Patrol 111
13.9.1 To Enable Policy Patrol 32-bit 111
13.9.2 To Enable Policy Patrol 64-bit 111

14 Troubleshooting 112

14.1 Knowledge Base 112
14.1.1 No Signatures are Being Added..... 112
14.1.2 My Sent Items in Outlook are not Being Updated..... 113
14.1.3 User Merge field is not Working..... 113
14.1.4 I Cannot Enter Licenses or Browse to Files or Folders.....113
14.1.5 How Can I Copy the Configuration to Another Machine?.....114
14.2 Send Support Files 114
14.3 Contacting Red Earth Software 114

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'.

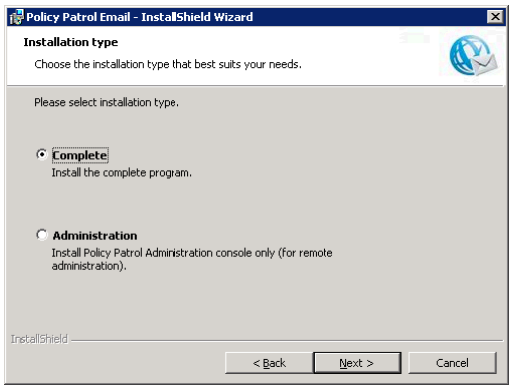
To install Policy Patrol follow the next steps:

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.

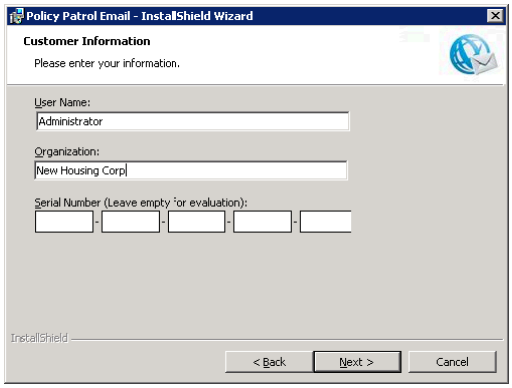
2. In the Welcome screen, click **Next**.

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

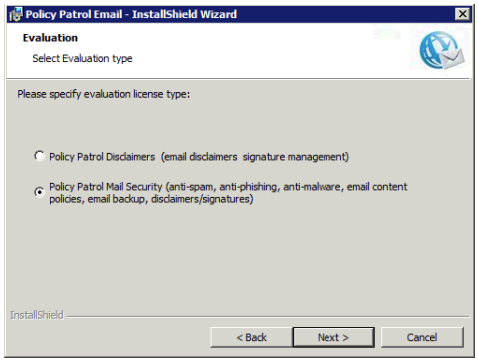
4. Select the installation type. If you select **Complete**, the complete program will be installed. If you only wish to install the Administration console (for remote administration), select **Administration**.



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**.

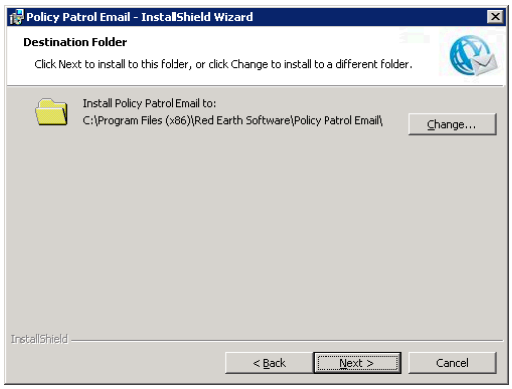


Tip

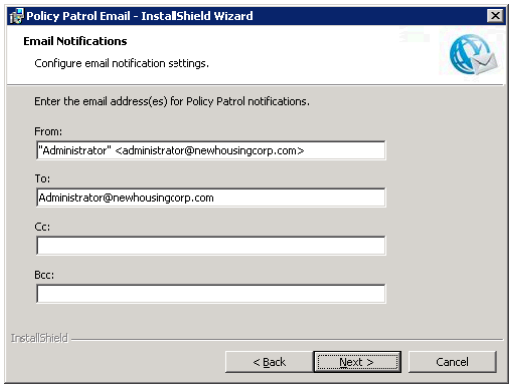
If you are evaluating Policy Patrol and later wish to try out a different Policy Patrol edition follow the next steps: After installation, open the Policy Patrol Administration console and go to **<server name>** > **Security** > **Licenses**, select the license and click **Remove**. Policy

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**.

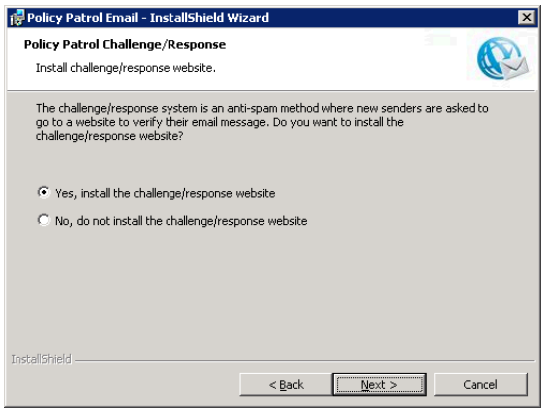


8. Specify the email notification settings. Enter the From:, To:, Cc: and Bcc: fields for the Policy Patrol notification emails. Policy Patrol notification emails inform you about evaluation expiry dates, licensing issues and new updates to the program. The From: display name is pre-configured as Administrator,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

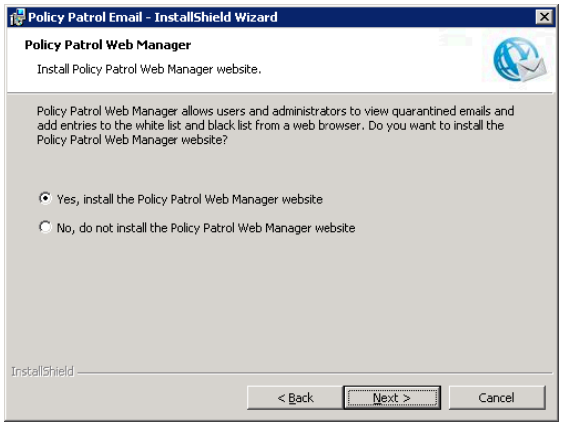


9. Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected **No, disable spam filtering**, continue to step 12.

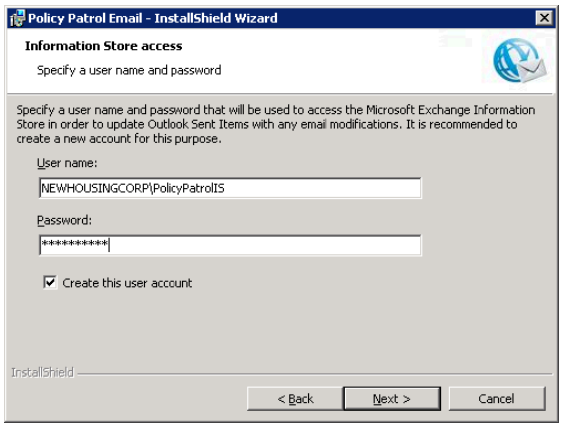
10. **If you selected to enable spam filtering**: Select whether you wish to install the challenge/response website. This website is needed if you wish to make use of the challenge/response system that asks new senders to go to a website and verify their email in order for the message to be delivered.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



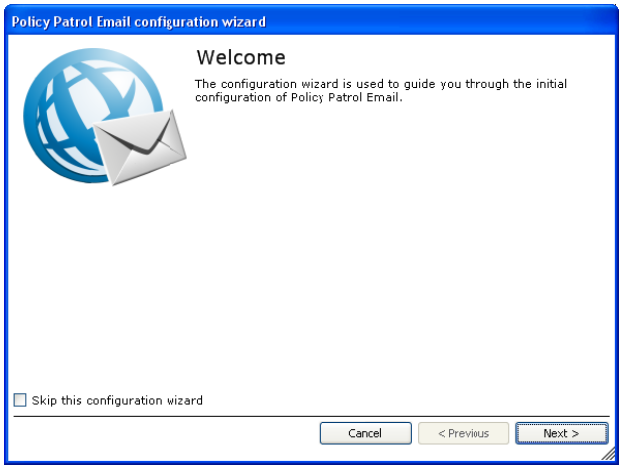
12. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please 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.

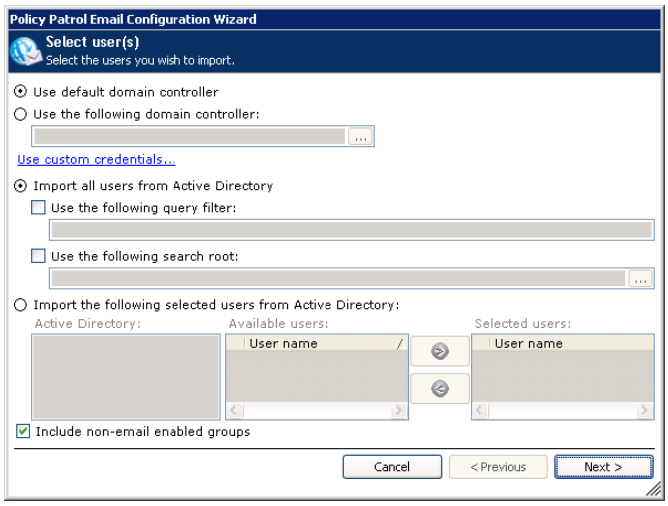
14. When the installation wizard has finished copying the files, click **Finish**.

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

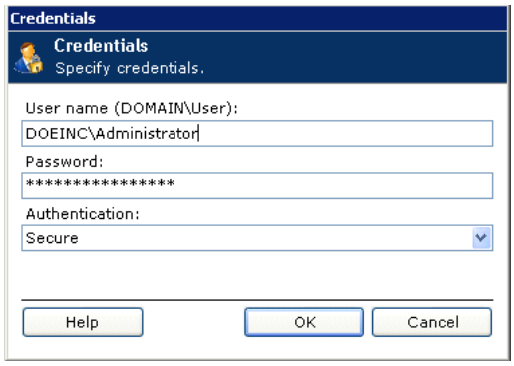


16. Specify the location from where you would like to import your users (Active Directory, Lotus Domino or Manual input). For more detailed information, consult chapter 4. Click **Next**. (Note: the 64-bit version only includes the Active Directory and Manual Input options.)

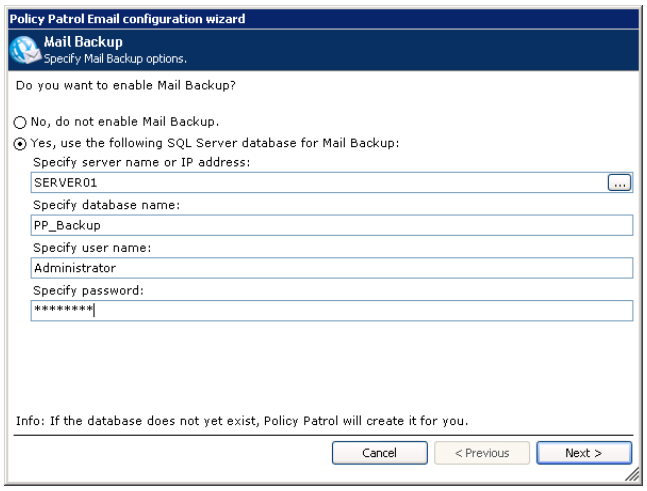
17. Specify the server or domain controller and select the users that you wish to license. You can either license all users or you can select only certain users to be licensed. For more information on the different options, consult chapter 4. Click **Next**.



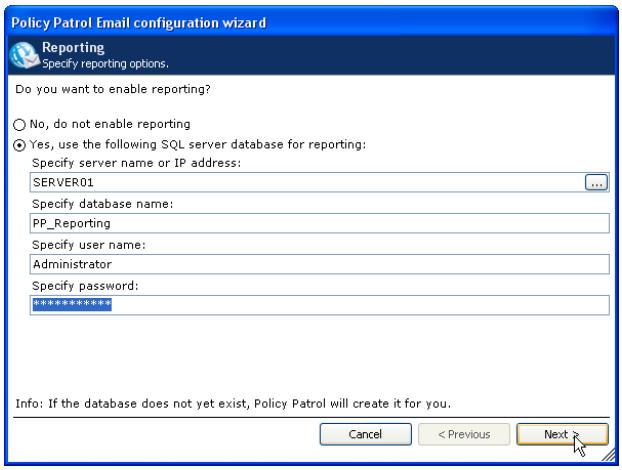
If you need to use a different user account than the account you are logged on with in order to retrieve users (for instance, this can be the case if you need to retrieve users from a different Active Directory sub domain), click on **Use custom credentials**. A dialogue will appear where you can enter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



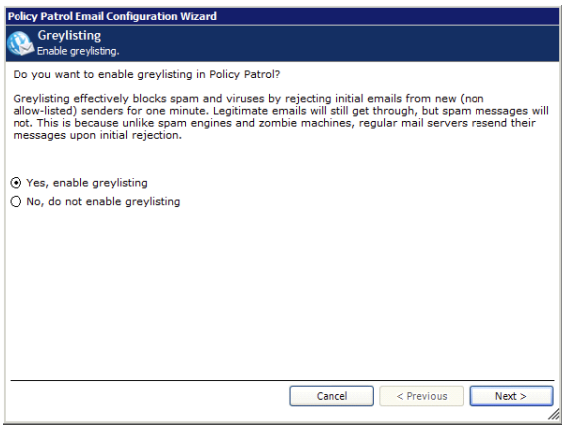
18. Select whether you wish to enable Mail Backup. If you enable Mail Backup you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically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

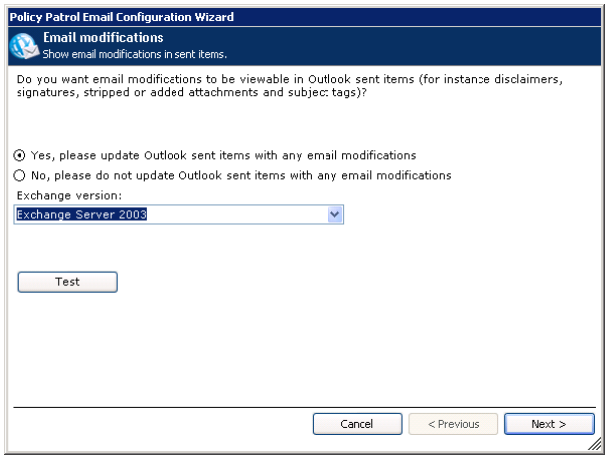


20. Select whether you wish to enable greylisting. Greylisting effectively blocks spam and viruses by initially rejecting messages from new, non white-listed senders for one minute, therefore allowing legitimate emails through without any user intervention, and blocking the non-legitimate emails. Select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

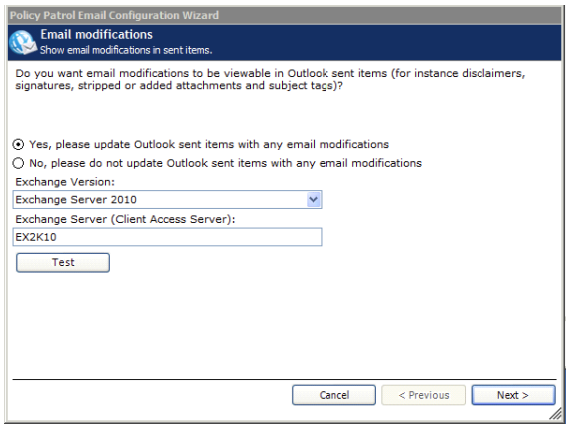


21. Select whether you wish to view email modifications in Outlook Sent items. If you select **Yes**, any modifications that are applied to outgoing emails by Policy Patrol, such as disclaimers, signatures, subject tags and adding or stripping attachments, will automatically show in Outlook Sent Items (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.

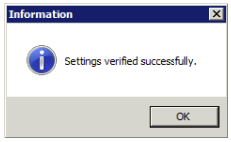
    If you have Exchange 2003: In 'Exchange version', Exchange Server 2003 should be selected.



    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.

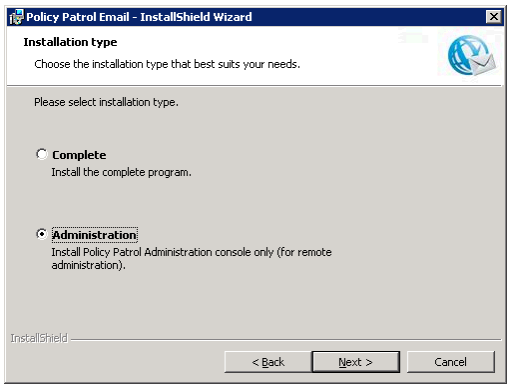
To install the Policy Patrol Remote Administration Console:

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.

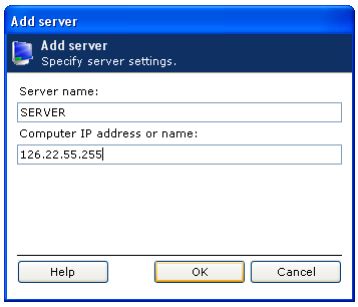
8. When the installation wizard has finished copying the files, click **Finish**.

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

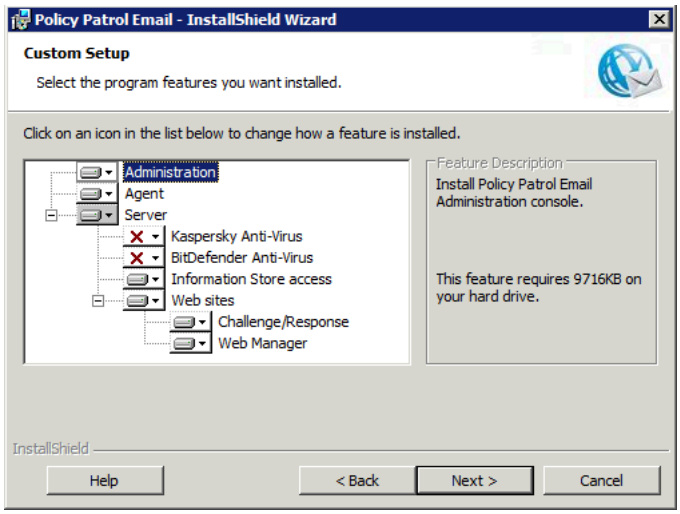
Policy Patrol installs a number of services on the machine. The following services are installed:

- ✓ 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)

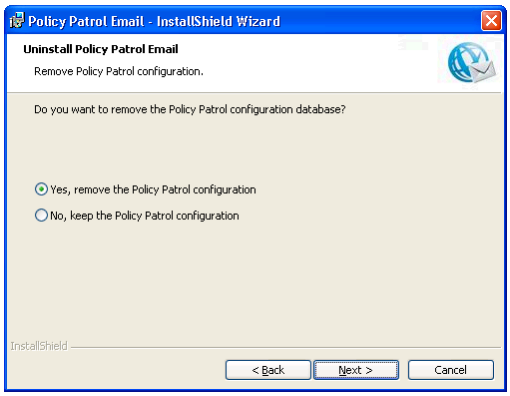
   When you have made your selections, click **Next**

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.

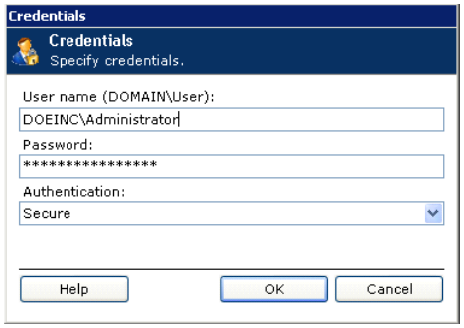
4.2 Import from Active Directory

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:

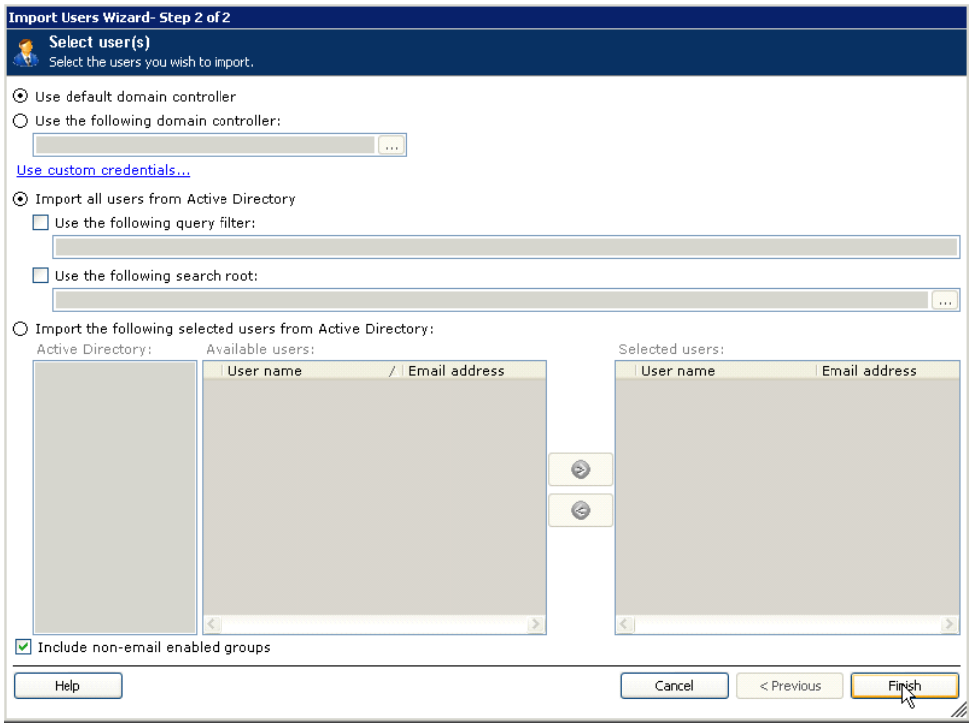
1. Go to **Settings** > **Users** and click on **Add...**.
2. In the Welcome screen, click **Next**.
3. Select **Active Directory** and click **Next**.
4. Leave the option **Use default domain controller** selected, or if you wish to retrieve users from another domain controller, select **Use the following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

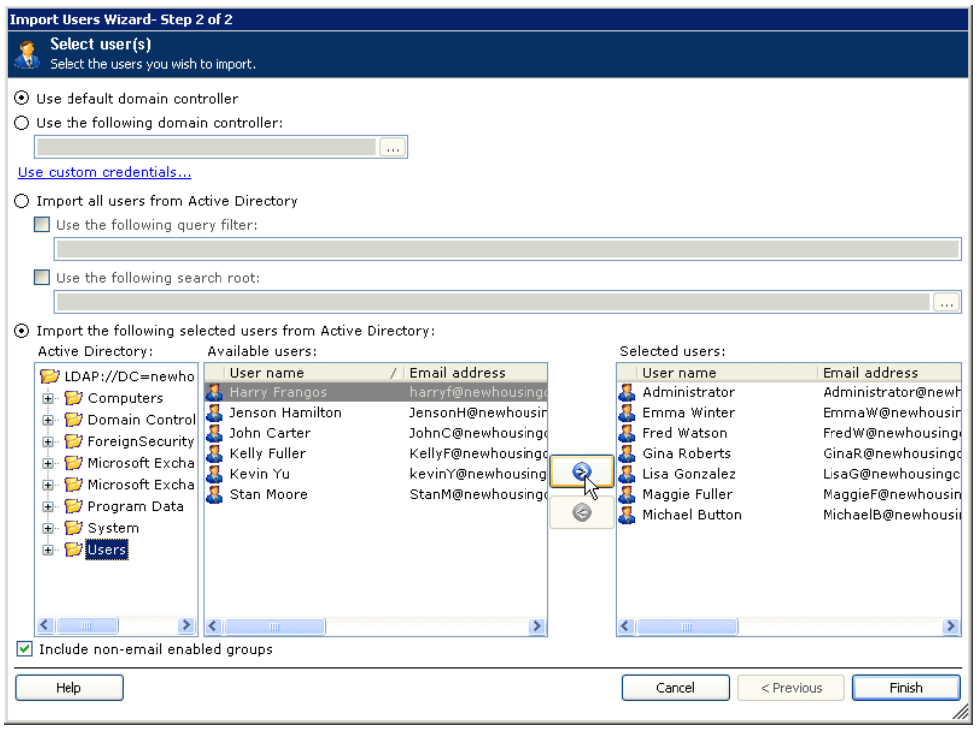
appear where you can enter your user name (DOMAIN\User), e.g. `DOEINC\Administrator`, the password and the authentication method. A number of authentication options are available, including Secure, Encryption, Anonymous, Secure Sockets Layer, etc. If you are not sure which Authentication option to choose, 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

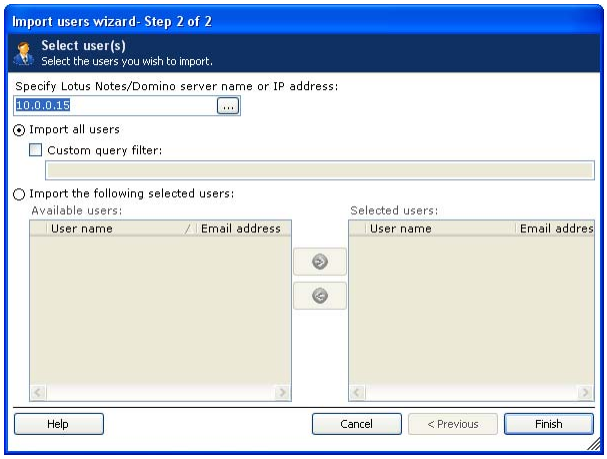
If you have Lotus Domino without Active Directory, you must retrieve users from Lotus Domino by following the next steps (this option is only available in the 32-bit version):

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

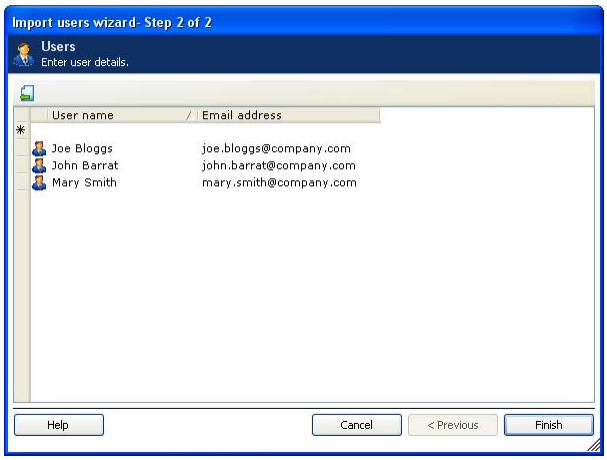
If you have another mail server without Active Directory, you must manually input your users by following the next steps:

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

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

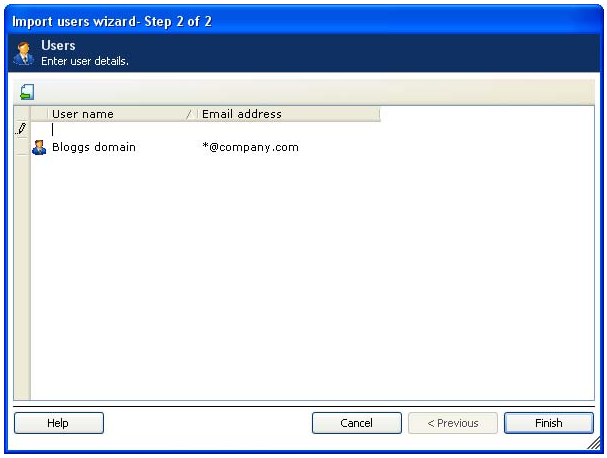
3. Select **Manual input** and click **Next**.

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

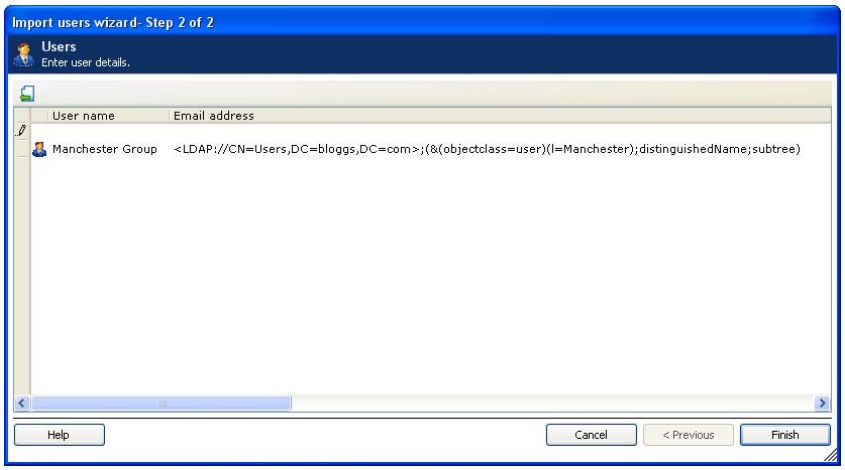
If you want to apply policies based on domain, you can configure a group that includes all users of a certain domain. To do this you must go to **Settings** > **Users**. Click on **Add**. Click **Next** in the Welcome screen, select **Manual input** and click **Next**. Now enter the group name in the '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

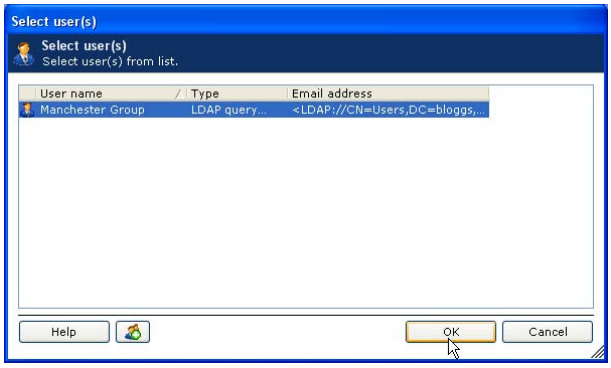
Note that the LDAP query must not exceed 120 characters.

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.

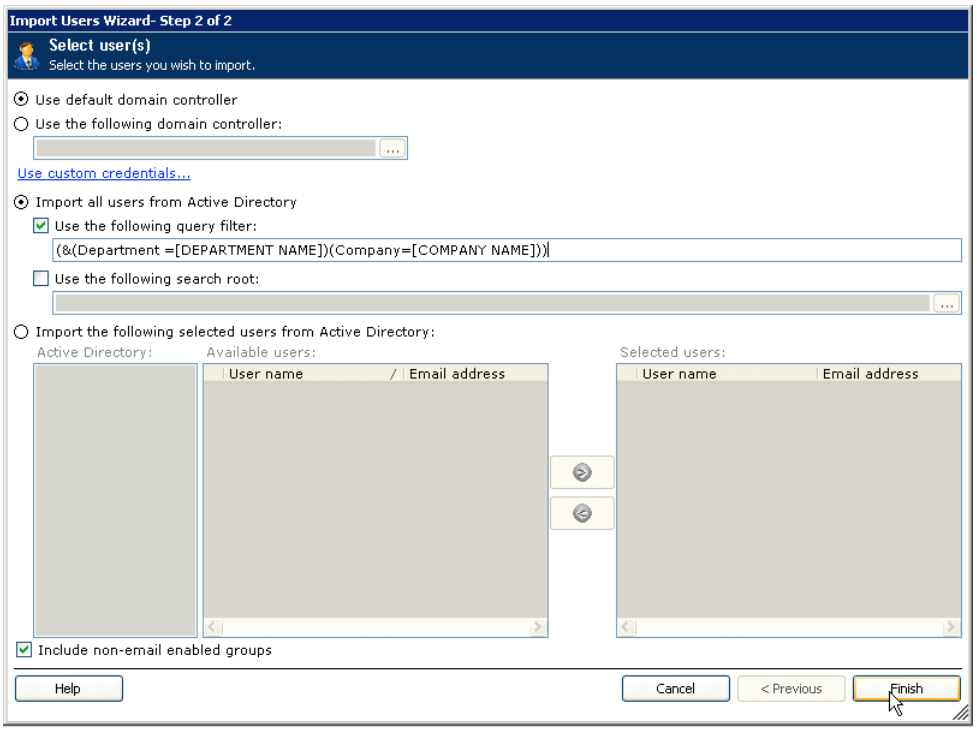
When you are ready, click **Finish**. The group name (i.e. Manchester Group) will now appear as a user when selecting users in a policy. By selecting the user 'Manchester Group' you will apply the policy to all users that are found by the query.



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'.

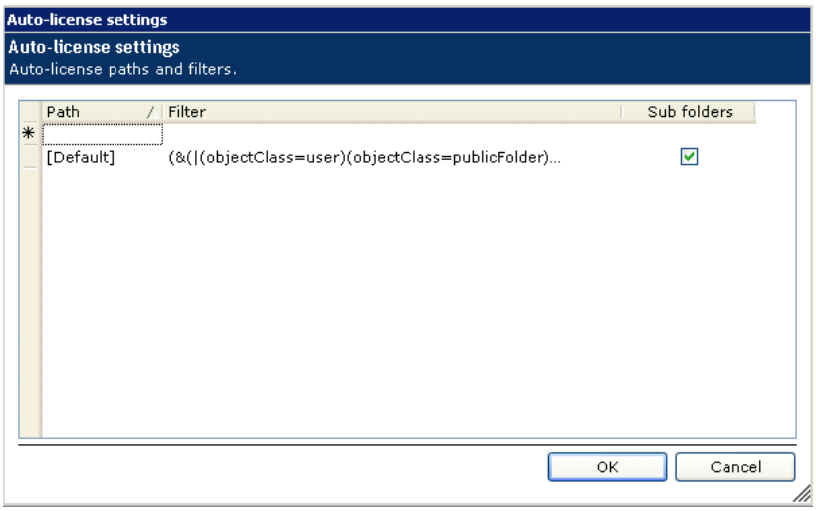
4.6 Editing Licensed Users

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 Signatures

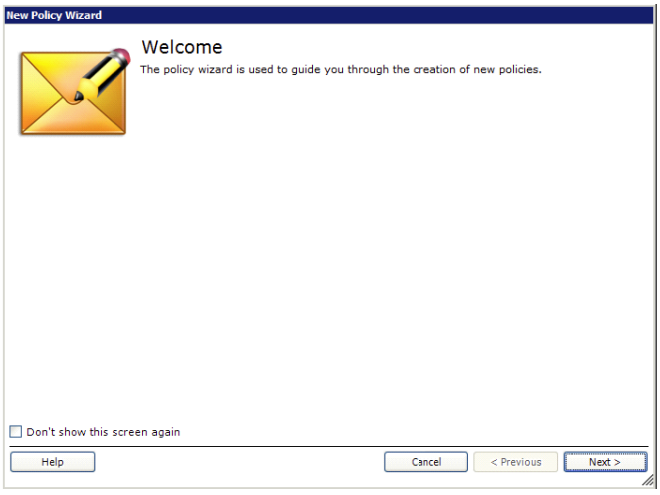
Policy Patrol allows you to add email disclaimers, personalized email signatures and HTML Stationery to your emails. This chapter describes how to configure the disclaimer, email signature and HTML stationery policies.

5.1 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.**



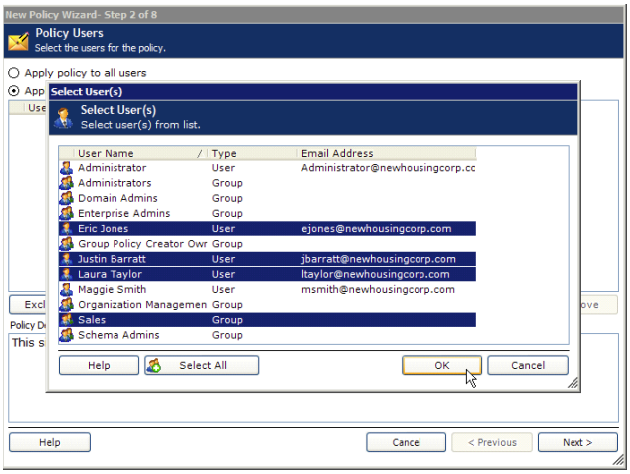
The policy wizard will now guide you through the different steps described below.

? 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.

5.1.1 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**.

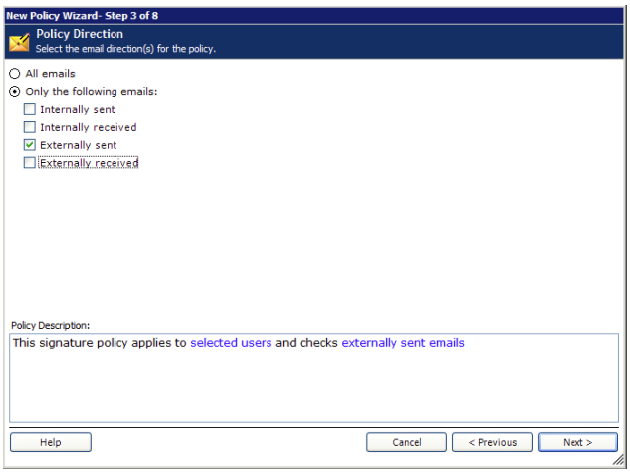


Tip

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).

5.1.2 Step 2. Policy Direction

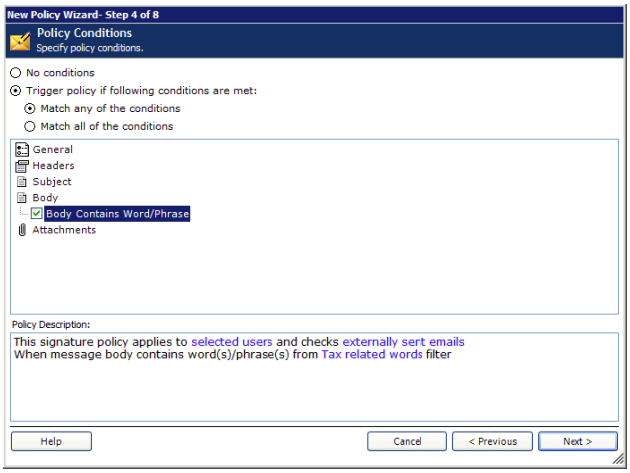
Specify whether you wish to apply the policy to all messages or only internally sent and/or received messages, and/or externally sent and/or received messages. Remember that Policy Patrol can only apply policies to internal messages if you have installed Policy Patrol on an Exchange Server machine. Click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



5.1.3 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.



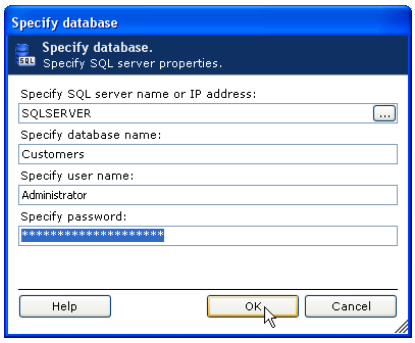
  ☑ **Message is of sensitivity**: Specify whether the message should be Normal, Personal, Private and/or Confidential.



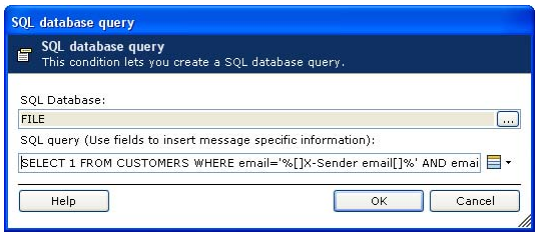
  ☑ **Message is DSN report**: Specify whether the message should be a Success, Delay, Failure notification, or Other report (report without status code).

> 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

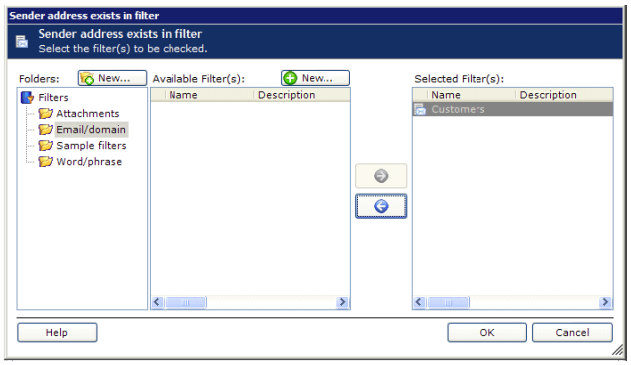
%[]Message field[]% = Message field that you want to match in the SQL table column

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 <> ''
```

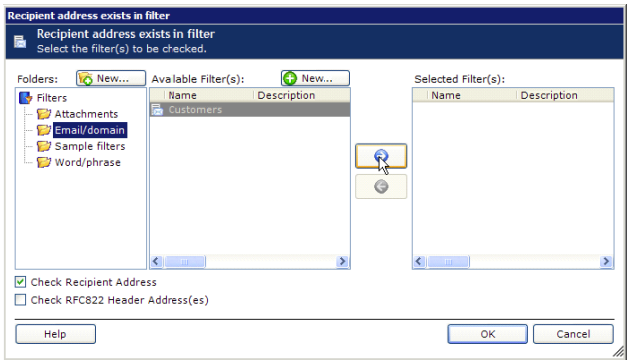
- **Headers**

☑ **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).

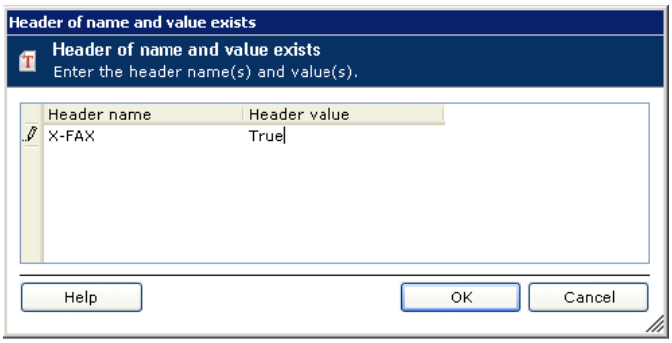


> **Note**
>
> The predefined filters folder contains the Email block list and Email allow list filter. These lists are configured from Anti-spam > Block/Allow. If you wish to handle spam messages via the policies you can select these filters if you wish.

☑ **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)**.

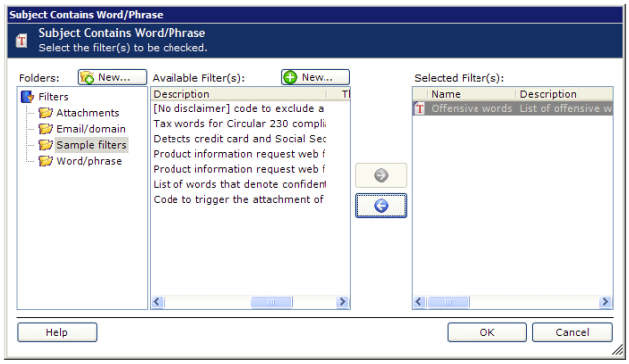


☑ **Header of name and value exists**: Enter the header name and value that Policy Patrol must search for.



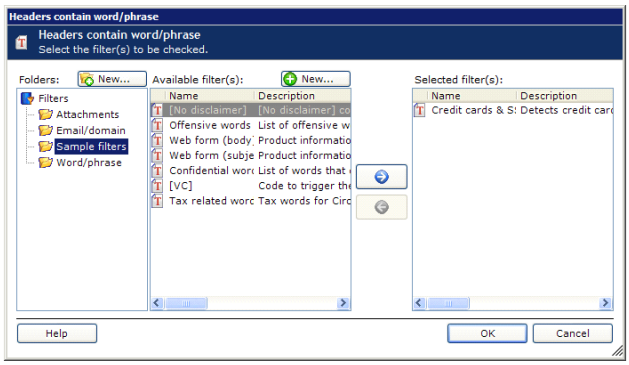
- **Subject**

☑ **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.



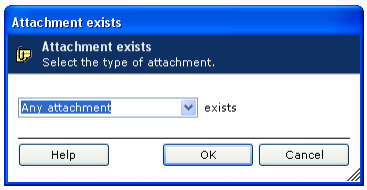
- **Body**

☑ **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).

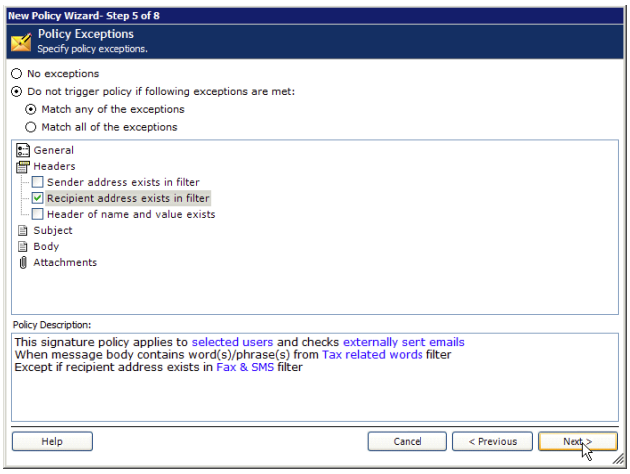


> Note
>
> Inline attachments are pictures or objects that have been inserted in the email message itself. Non-inline attachments are files that have been attached to the message.

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

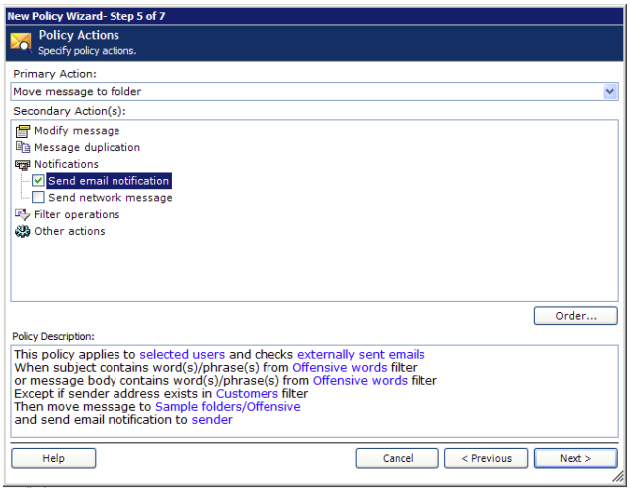
5.1.4 Step 4. Policy Exceptions

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**.



5.1.5 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.



5.1.5.1 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.

5.1.5.2 Secondary Actions

The following secondary actions are available:

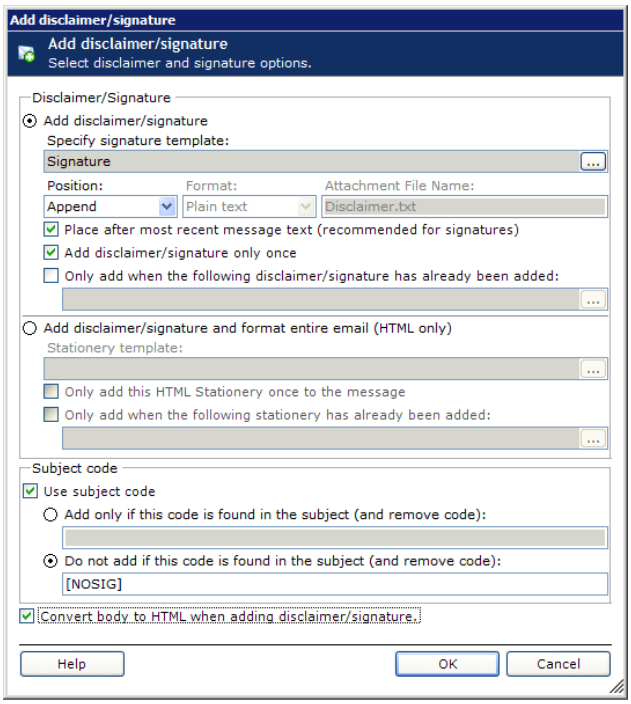
- **Modify message**

  ☑ **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

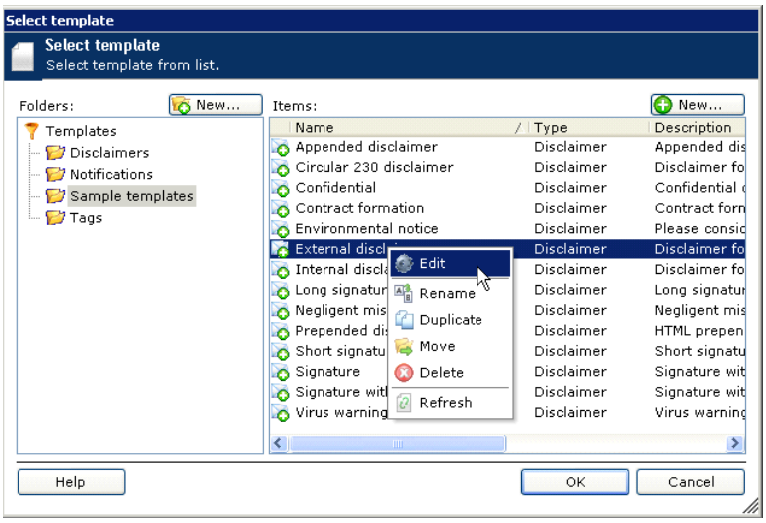
signature. The option **Add disclaimer/signature** allows you to add a block of text at the bottom or top of an email (or below the most recent message text), but it does not change the actual email body text. The option **Add disclaimer/signature and format the entire email (HTML only)** allows you 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).

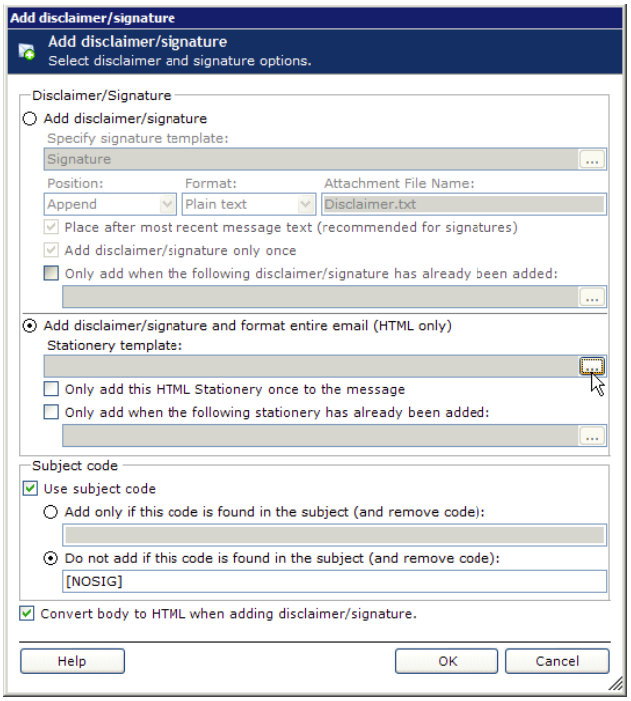
Tip

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.

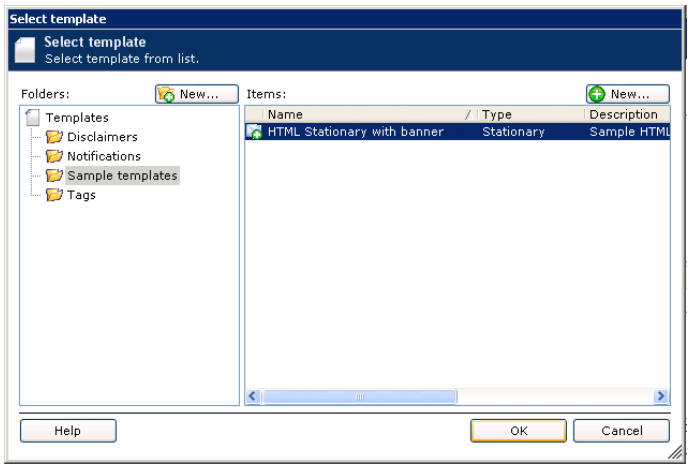
❑ Add disclaimer/signature and format entire email (HTML only)

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.

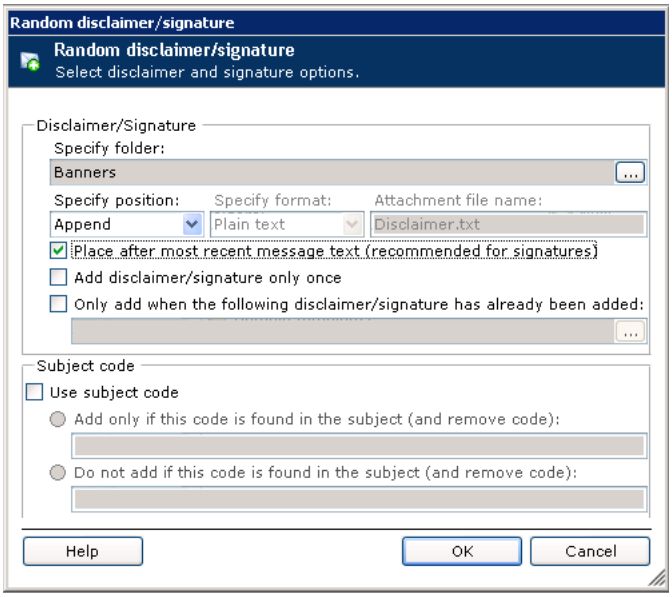
If you do not wish to add the disclaimer/signature/stationery if a certain code is found in the subject, select the option **Do not add if this code is found in the subject (and remove code)**. For instance, you can instruct users to enter the code `[No disclaimer]` in the subject if they do not want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

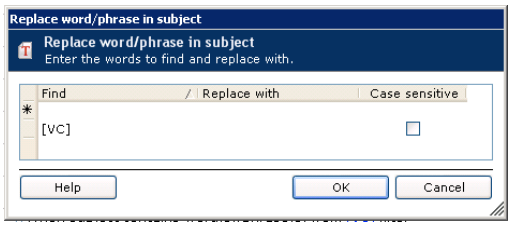
  If you wish to convert plain text emails to HTML so that the HTML signature or stationery can be added, select the option **Convert body to HTML when adding disclaimer/signature**. This is especially useful for emails sent from mobile devices: Since all mobile devices send emails out in plain text format, 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.

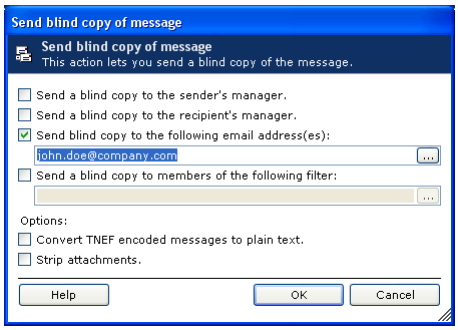
Note: this action is only required if you are adding a vCard to the message and only wish the vCard to be added/suppressed if a code is found in the subject. If you wish to add/suppress a disclaimer/signature if a code is found in the subject, this can be configured form the **Add disclaimer/signature**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



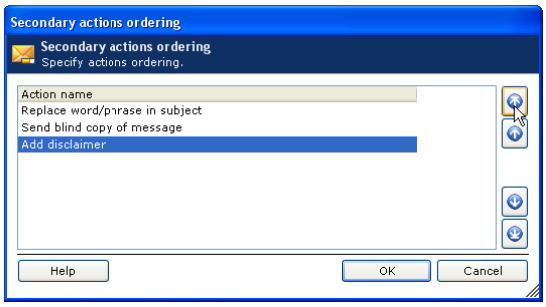
Note

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**.

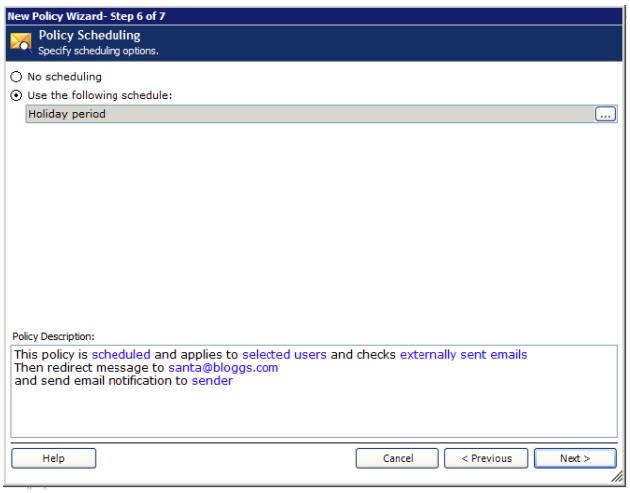
5.1.5.3 Ordering of Secondary Actions

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.



5.1.6 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'.

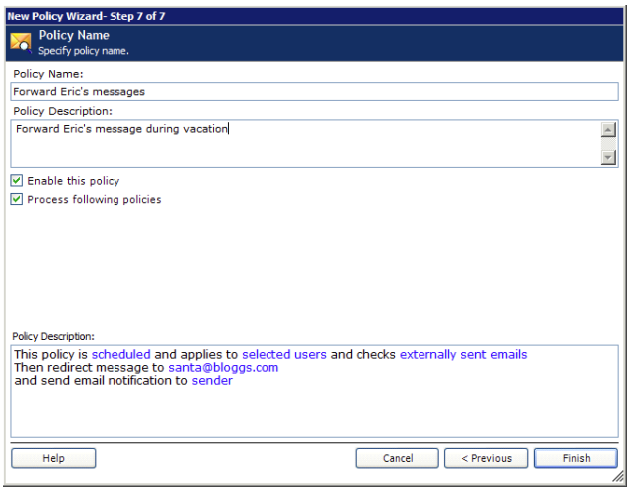


Tip

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

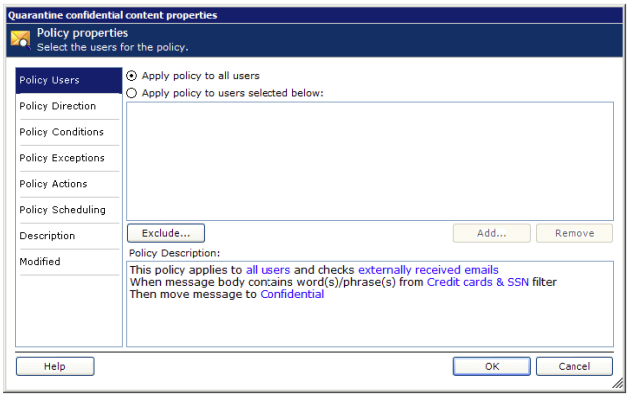
5.1.7 Step 7. Policy Name

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.



5.2 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**.



5.3 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>.

5.4 Moving Policies

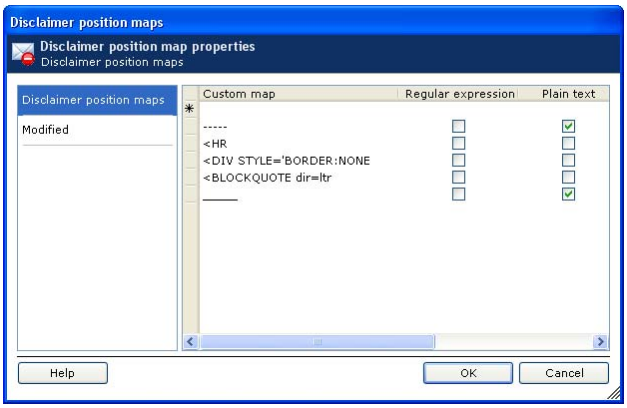
To move a policy to a different folder, right click on the policy and select **Move**. Select the folder you wish to move the policy to and click **OK**. To create a new folder, click the **New...** button.



5.5 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.



5.6 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 13.3.3 Email Modifications.

Chapter

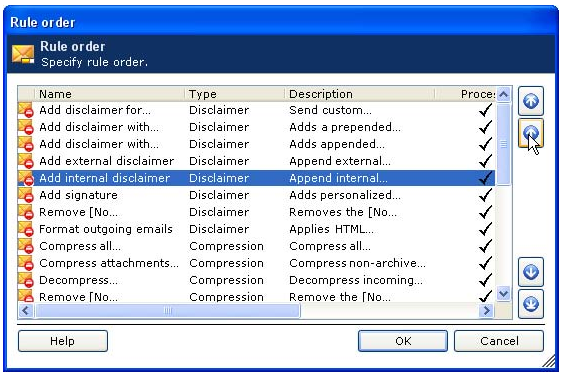
6

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.

6.1 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.

6.1.1 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.

6.1.2 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`.

6.1.3 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

7

Creating Filters

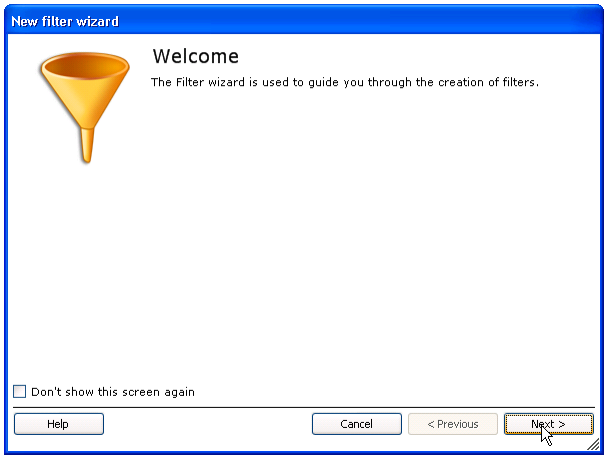
Filters are lists that Policy Patrol must check for. Policy Patrol includes Word/phrase, Attachment and Email/domain filters. This chapter explains how to create each type of Policy Patrol filter.

7.1 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**.

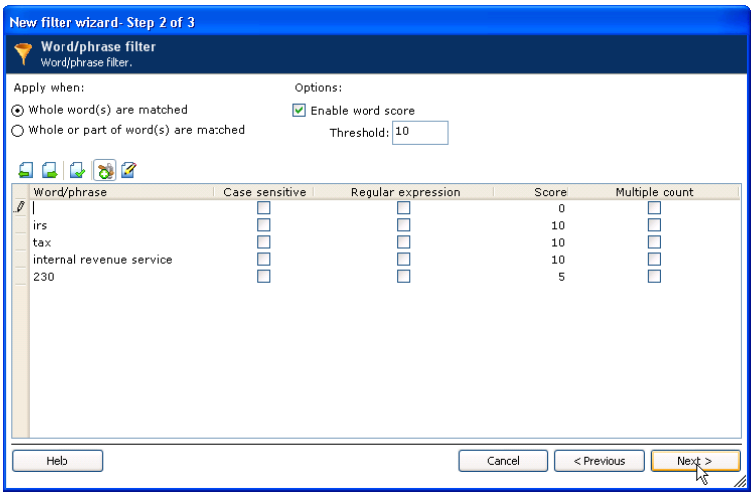
4. Enter the word(s) or phrases to be included in the filter. The following options are available:

   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.

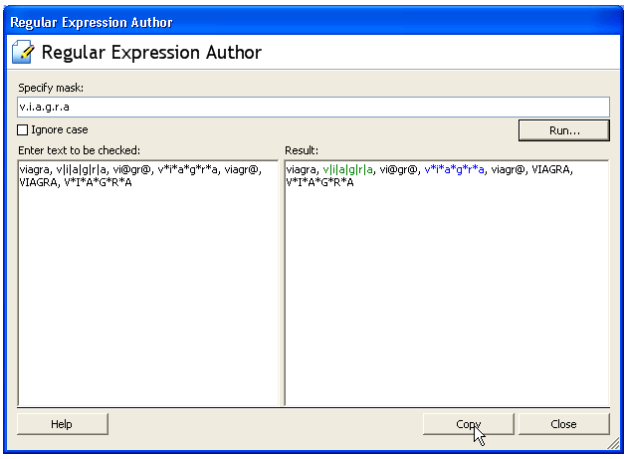


Note

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.

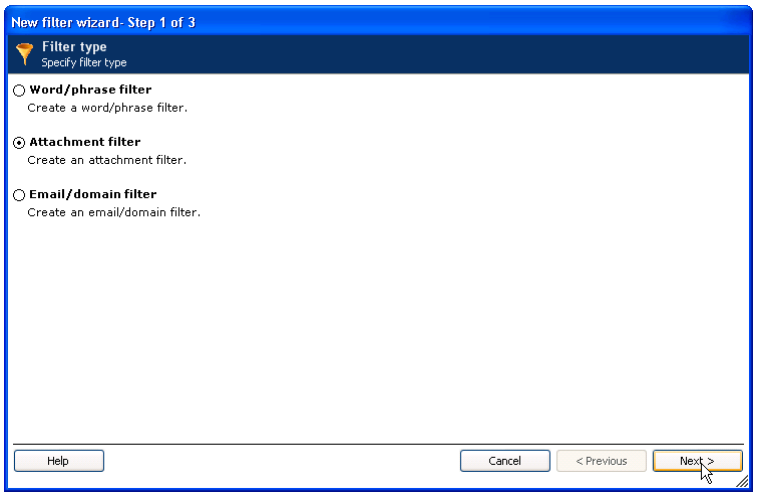
7.2 Creating an Attachment Filter

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:

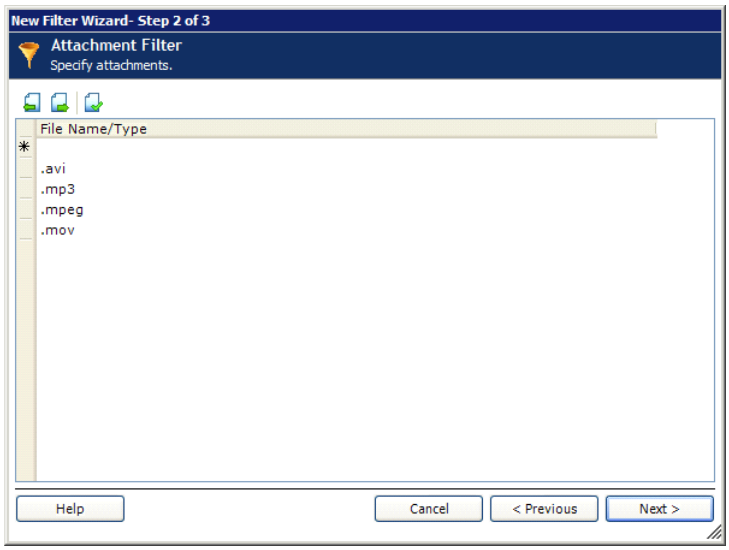
1. Go to **Settings** > **Filters**, select the appropriate folder and click **New...**.

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.

7.3 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:

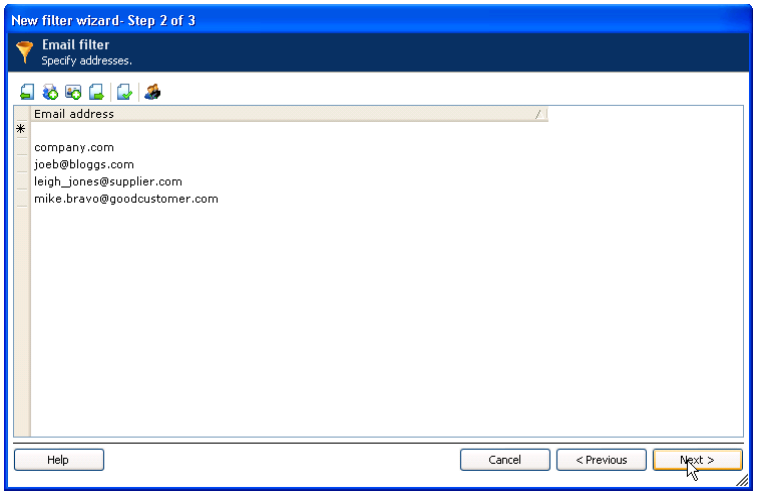
1. Go to **Settings** > **Filters**, select the appropriate folder and click **New...**.

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.

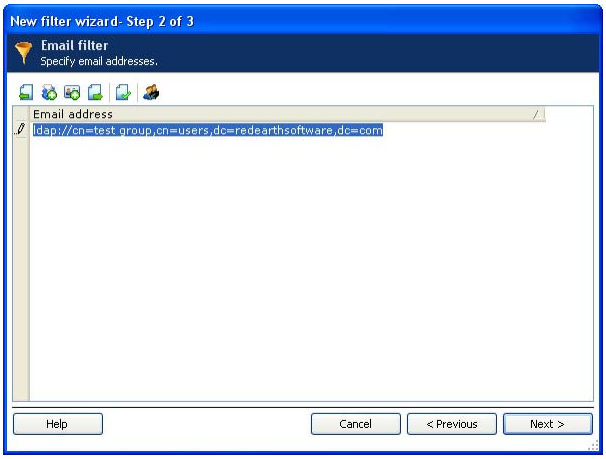
   You can import lists from .txt files by clicking on **Import**, browsing to the appropriate file and clicking **Open**. In the text file to import, each domain/email address should be entered on a separate line. To export the filter, click **Export**, enter a file name and select **OK**. If you want 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.

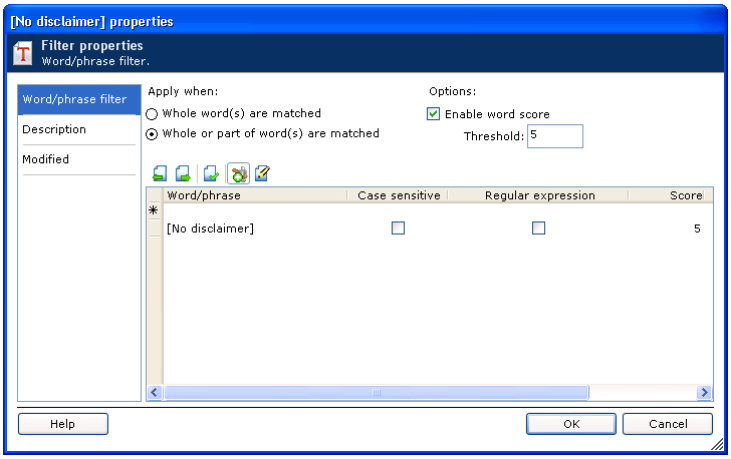
7.3.1 Active Directory Users in Email Filter

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.



7.4 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.

7.5 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>.

7.6 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.

7.7 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

8

Creating Templates

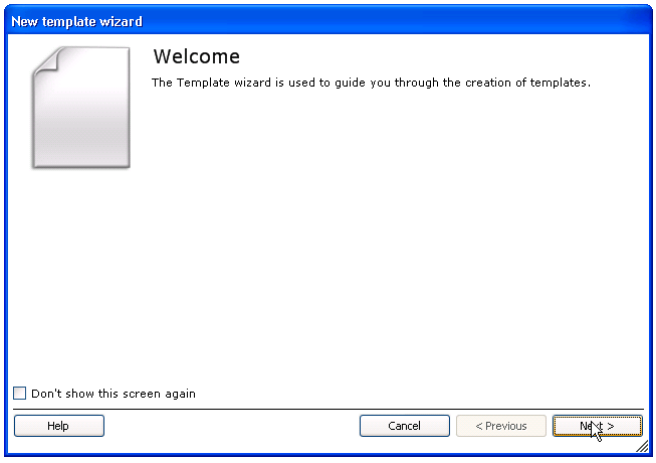
Templates are pre-configured texts that can be used in Policy Patrol. This chapter describes how to create notification, tag and disclaimer templates.

8.1 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:

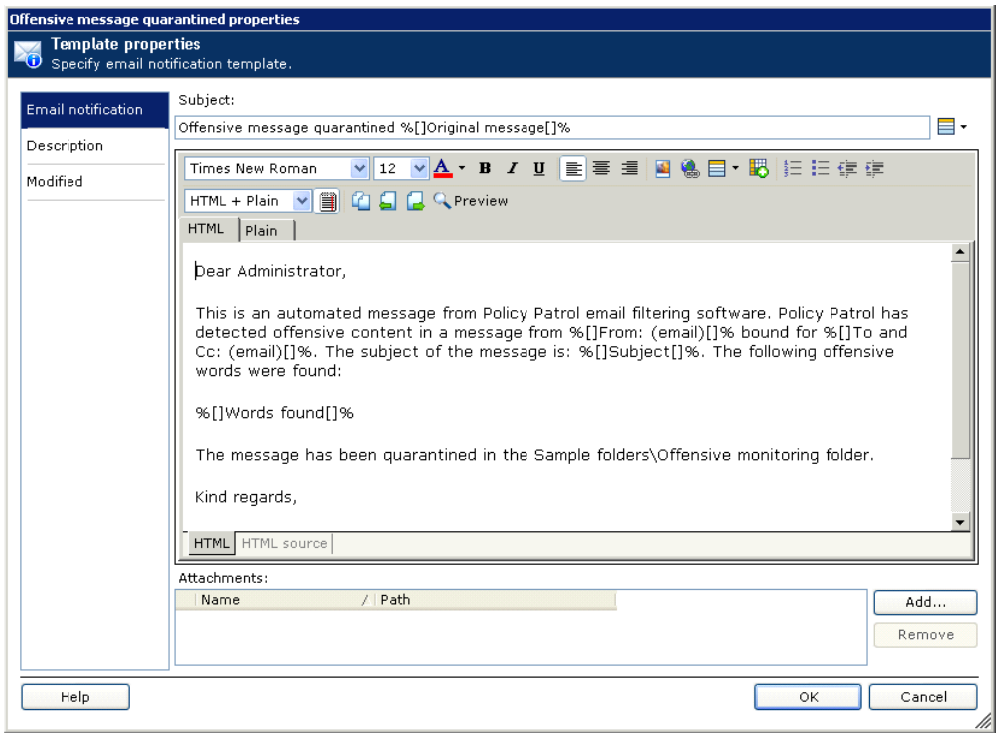
1. Go to **Settings** > **Templates**, select the appropriate folder and click **New...**.

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



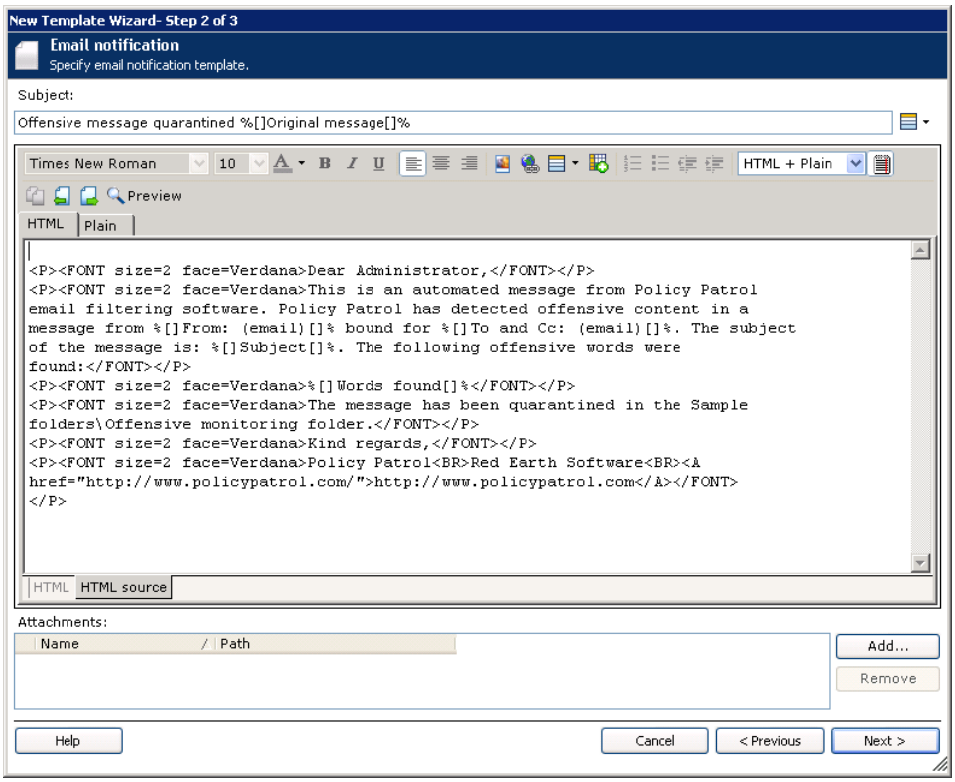
3. When asked which type of template you wish to create, select **Email Notification Template**. Click **Next**.

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

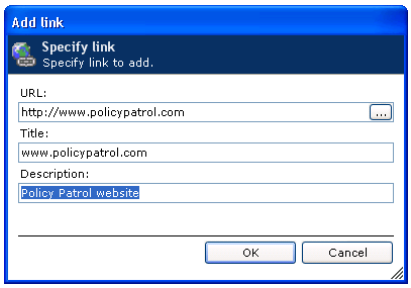
Note that if you enter the Original message field it is best to enter it in the subject since if you add it to the body of the HTML as well as the Plain text tab, the message will be added twice.

Tip

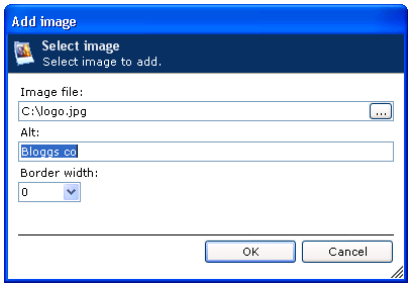
It is possible to manipulate Active Directory merge fields so that if not all users have the same Active Directory information, certain fields will not be shown for all users. For instance if some users do not have a cell phone number in their Active Directory properties, these fields can be hidden for 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.

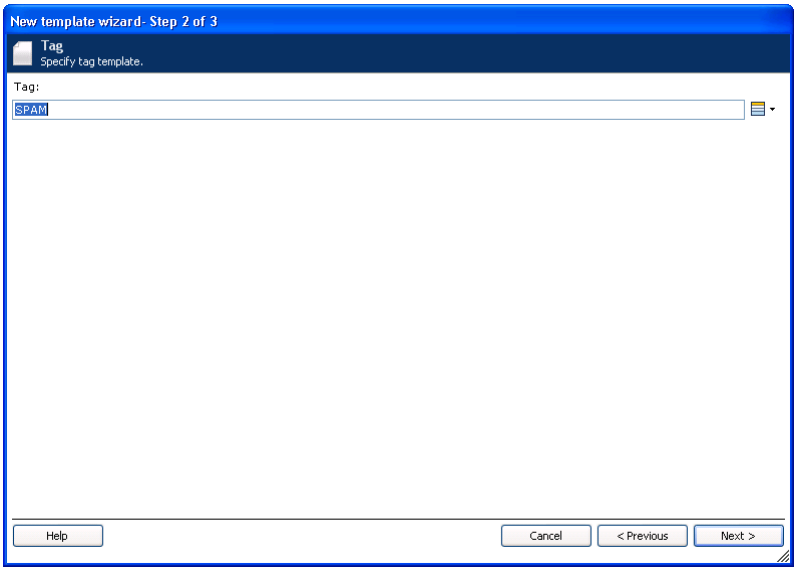
8.2 Creating a Tag Template

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.

8.3 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.

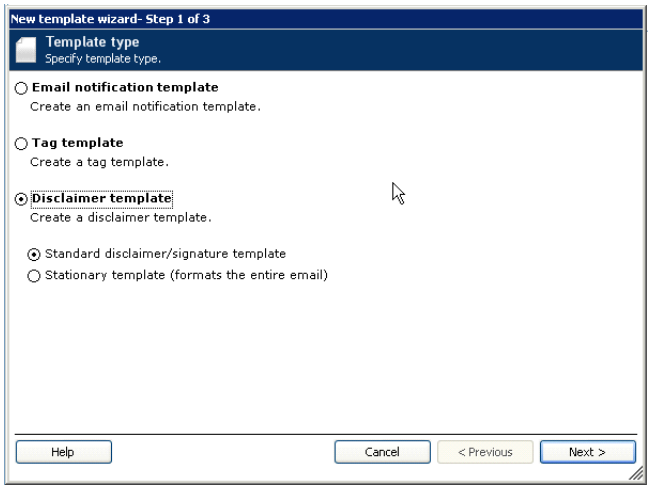
Stationery Template (formats the entire email): This template is used if you wish to add a disclaimer or signature and format the entire email, including the original body text. For instance if you wanted to format your emails like a web page, or you want to add your contact details in a column to the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

8.3.1 Creating a Standard Disclaimer/Signature Template

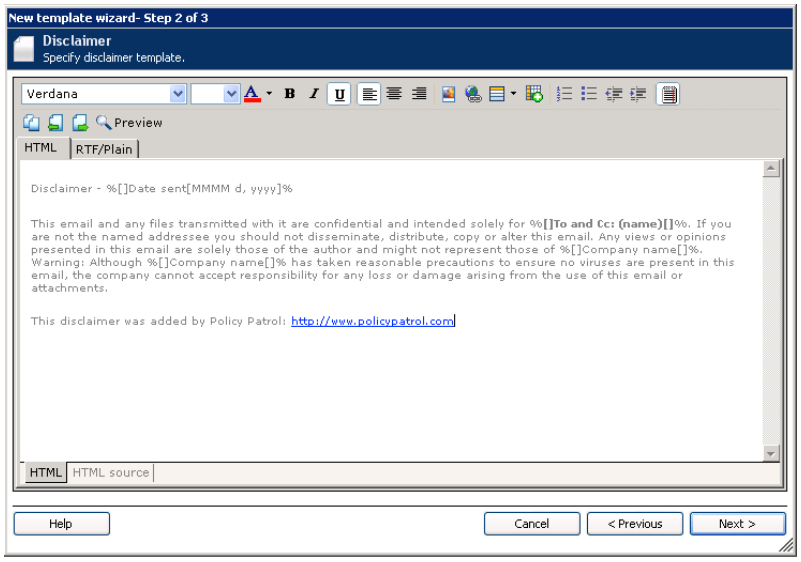
To create a standard Disclaimer/Signature template:

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..** .

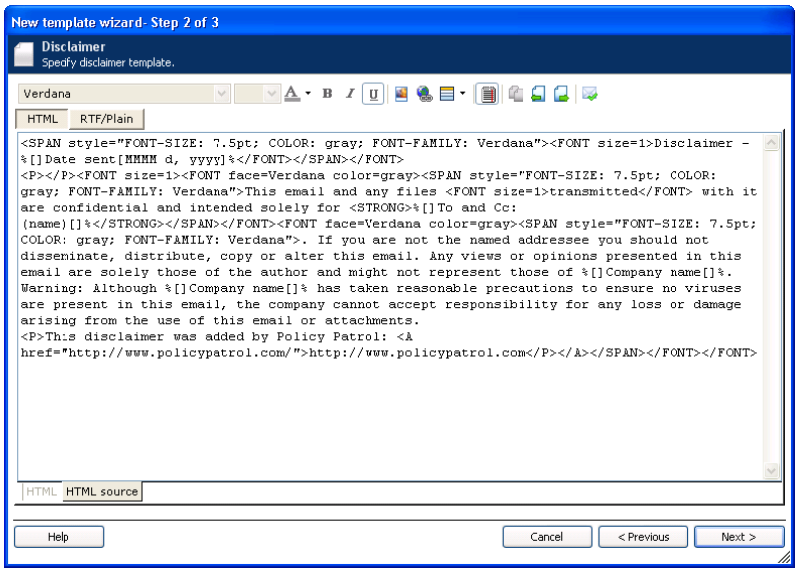


Note

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

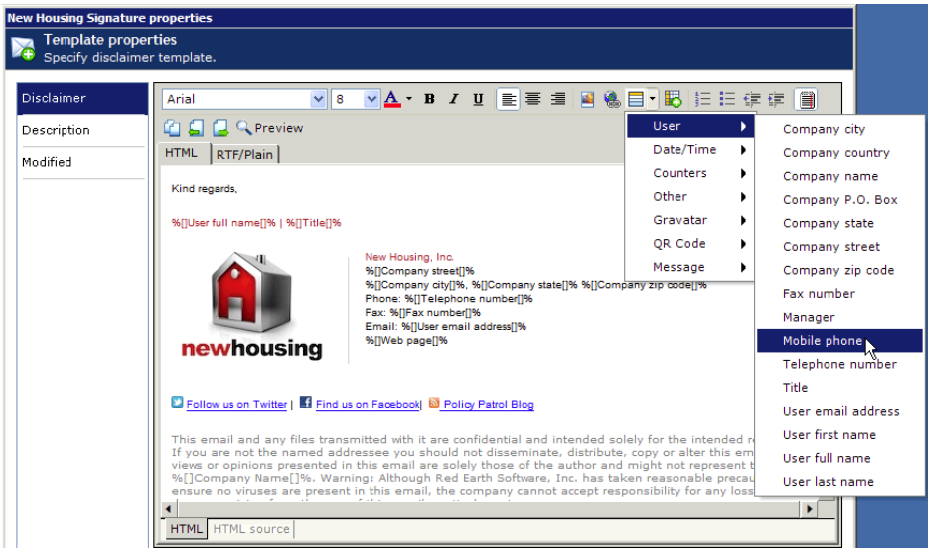
must always enter a disclaimer text in the RTF/plain text tab, even if you only send out HTML messages. However, you only need to enter your text once, since you can copy and paste the text from one tab to another by clicking on the **Copy to..** button.

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.

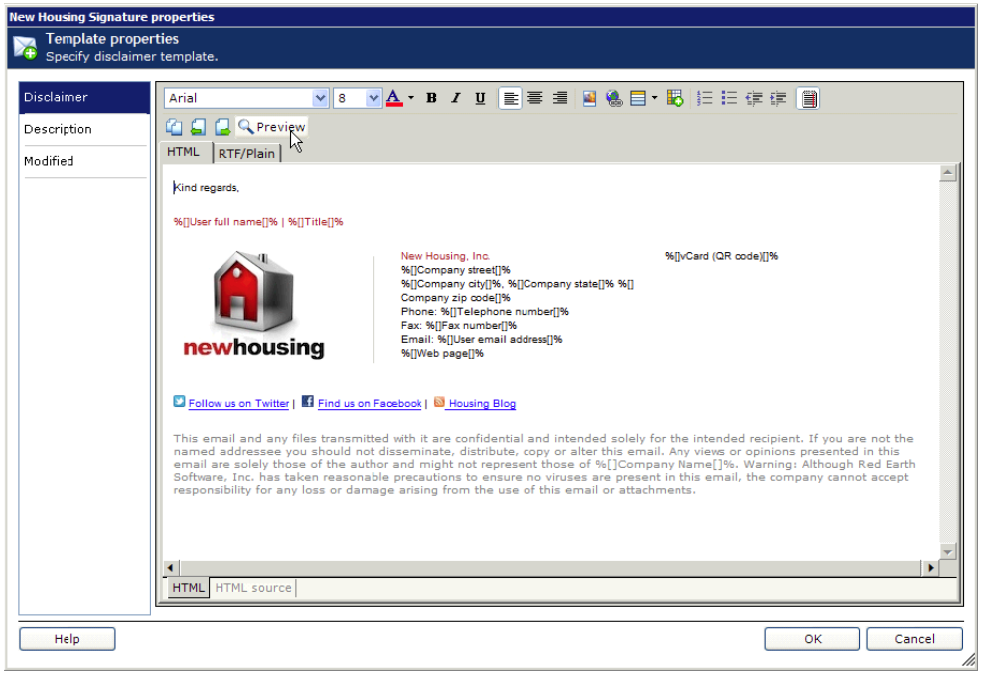


From the toolbar, you can select font, size, color, bold, italic, and underlined. You can add bulleted lists, numbered lists, indent and align text.

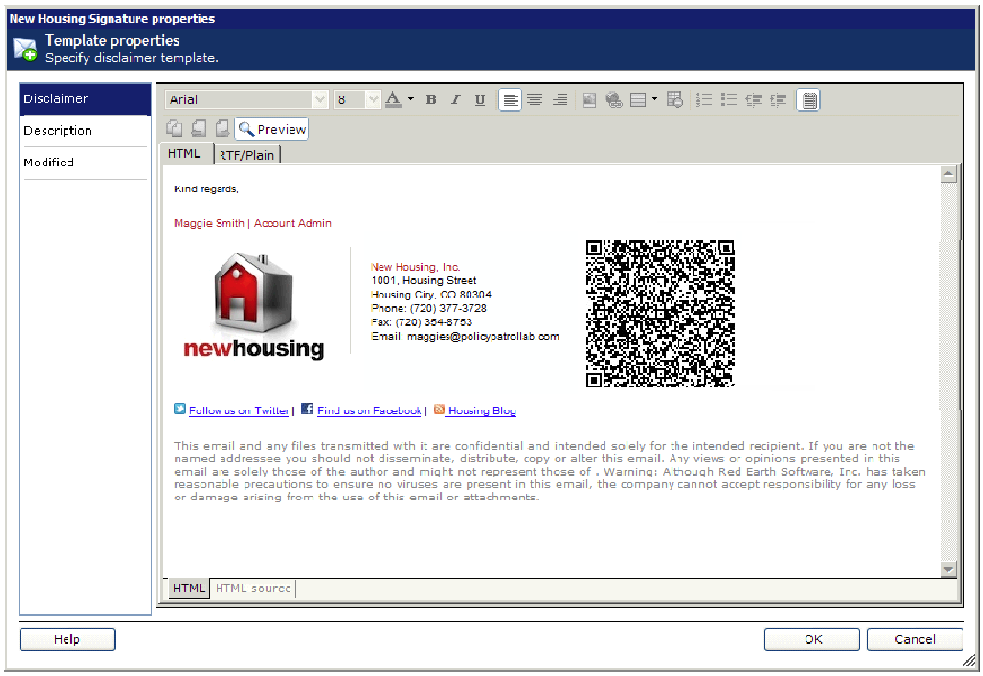
You can insert merge fields by clicking on the **Insert Field** icon  and selecting the relevant field. For more information on the available fields, see the 'Fields' paragraph in this chapter.



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

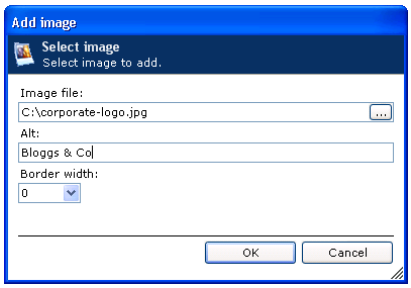
It is possible to manipulate Active Directory merge fields so that if not all users have the same Active Directory information, certain fields will not be shown for all users. For instance if some users do not have a cell phone number in their Active Directory properties, these fields can be hidden for 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.

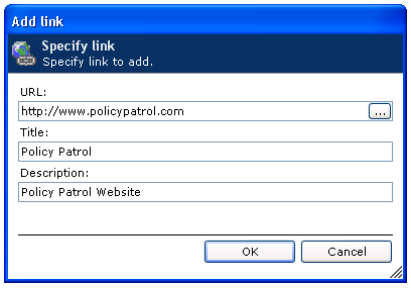
You can import texts from .txt and .html documents by clicking **Import**. Similarly, you can export the text to a .txt or .html file by clicking **Export**.

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'.

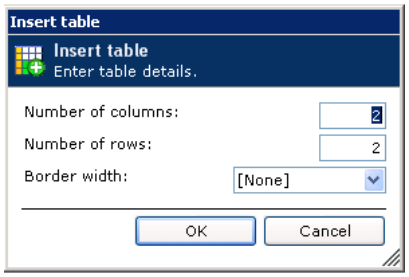


To add a link, click on the **Insert Link** button. In **URL:** enter the URL to link to. Enter the text to be displayed in **Title** and enter the description in **Description**.



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.

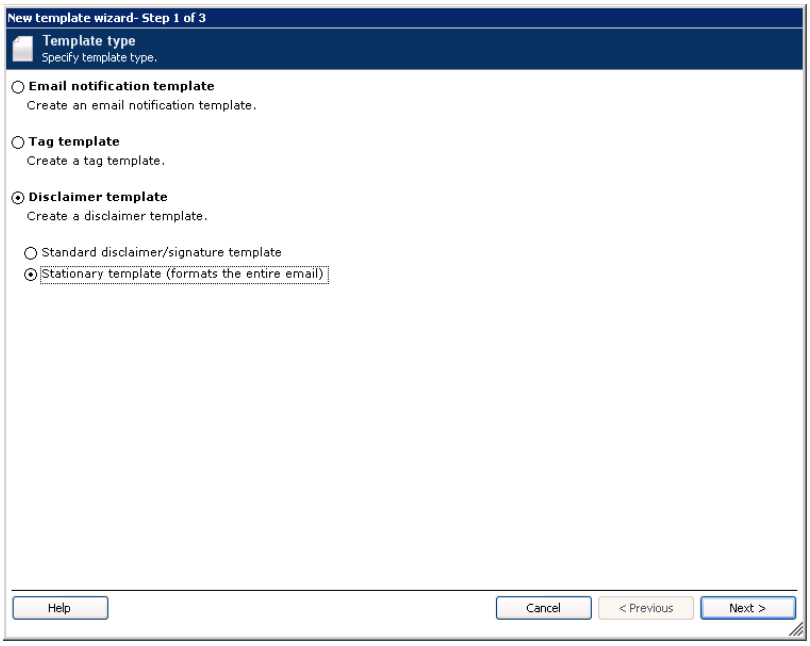
8.3.2 Creating an HTML Stationery Disclaimer Template

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)**.



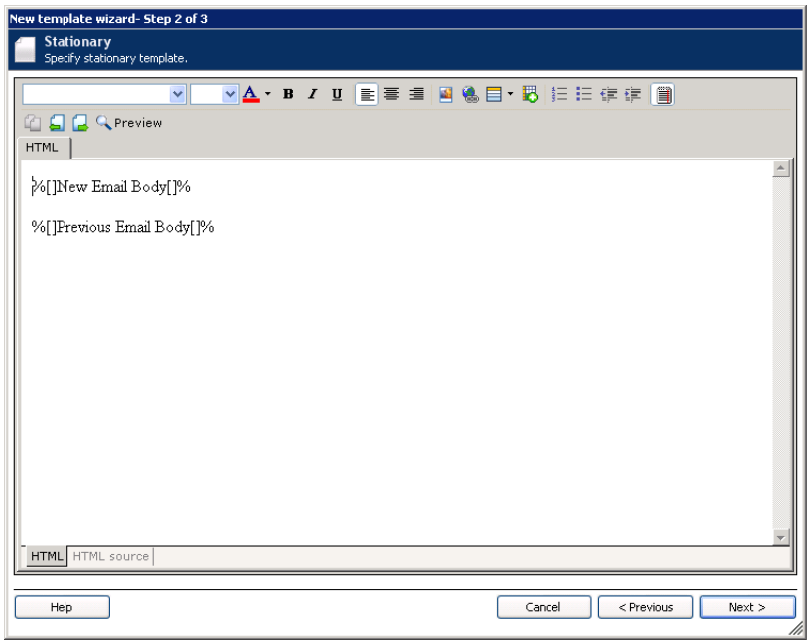
3. You will see two merge fields in the template:

   %[]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.

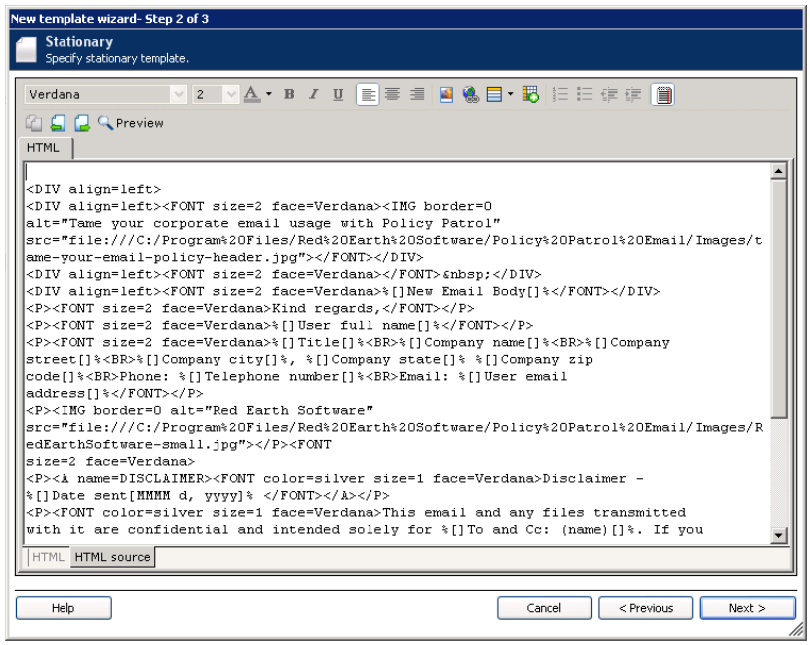
   %[]Previous Email Body[]%:This field will be replaced with the previous message text, i.e. the email text below the first message separator.

   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**.

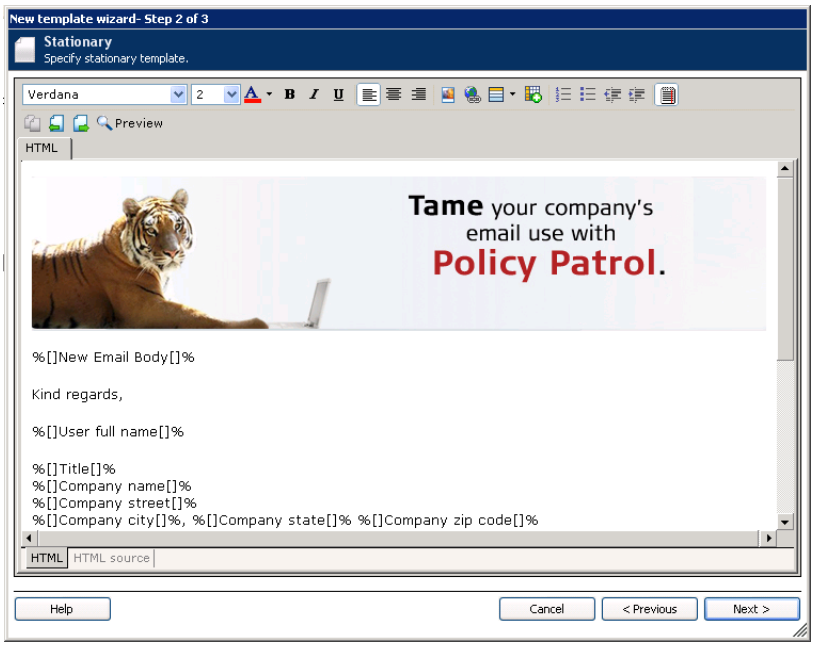


You can directly edit the HTML source by clicking on **HTML Source** at the bottom of the dialog.



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.

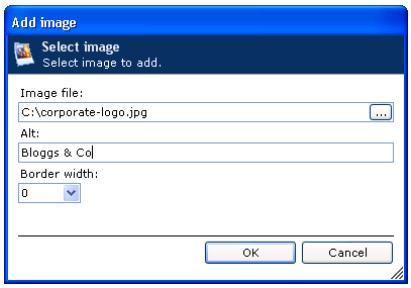
Tip

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'.

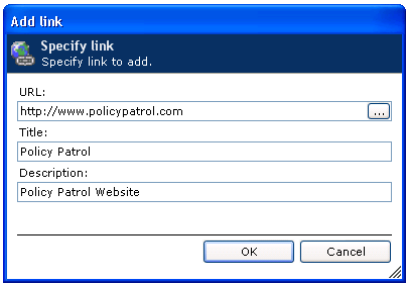
You can import texts from .txt and .html documents by clicking **Import**. Similarly, you can export the text to a .txt or .html file by clicking **Export**.

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'.

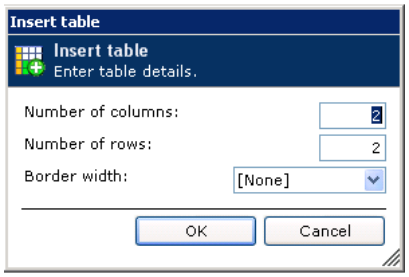


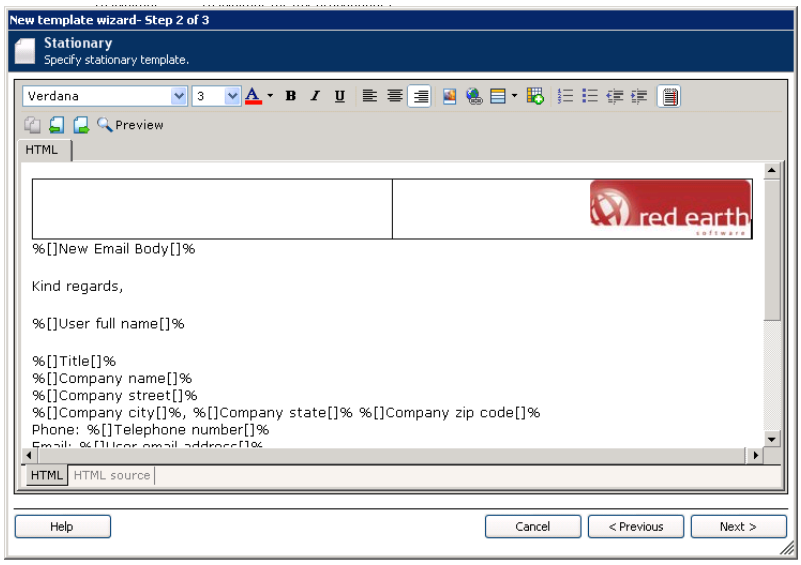
To add a link, click on the **Insert Link** button. In **URL:** enter the URL to link to. Enter the text to be displayed in **Title** and enter the description in **Description**.



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**.



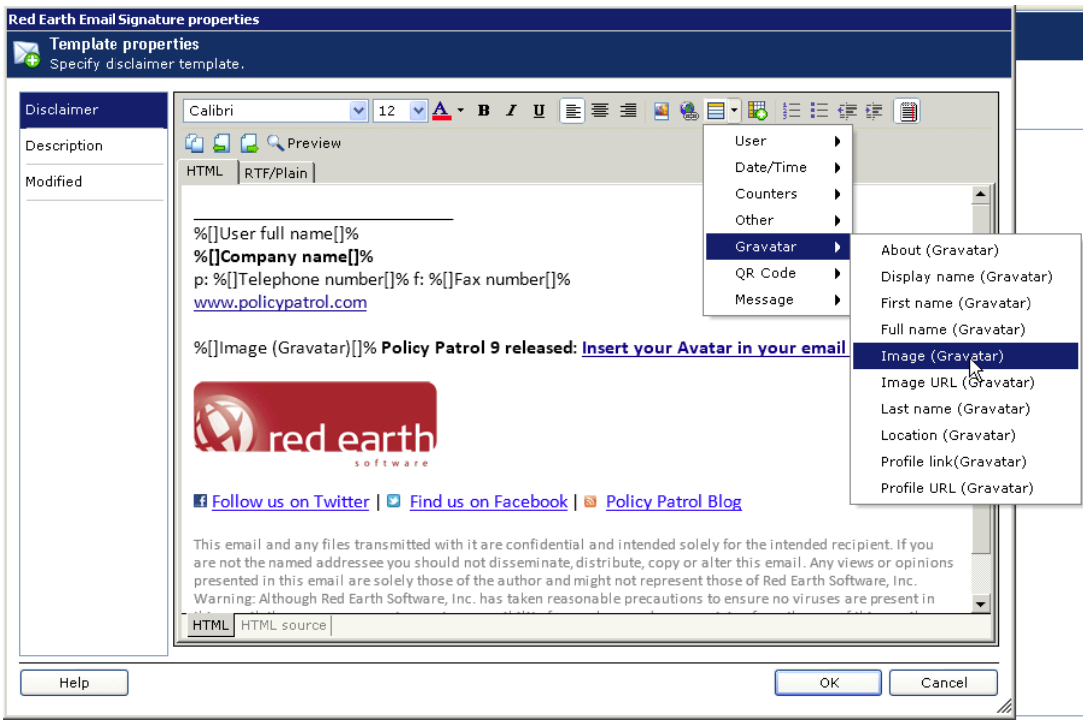


4. Enter the template name and a description. Click **Finish** to create the template.

8.4 Inserting an Avatar in the Email Signature

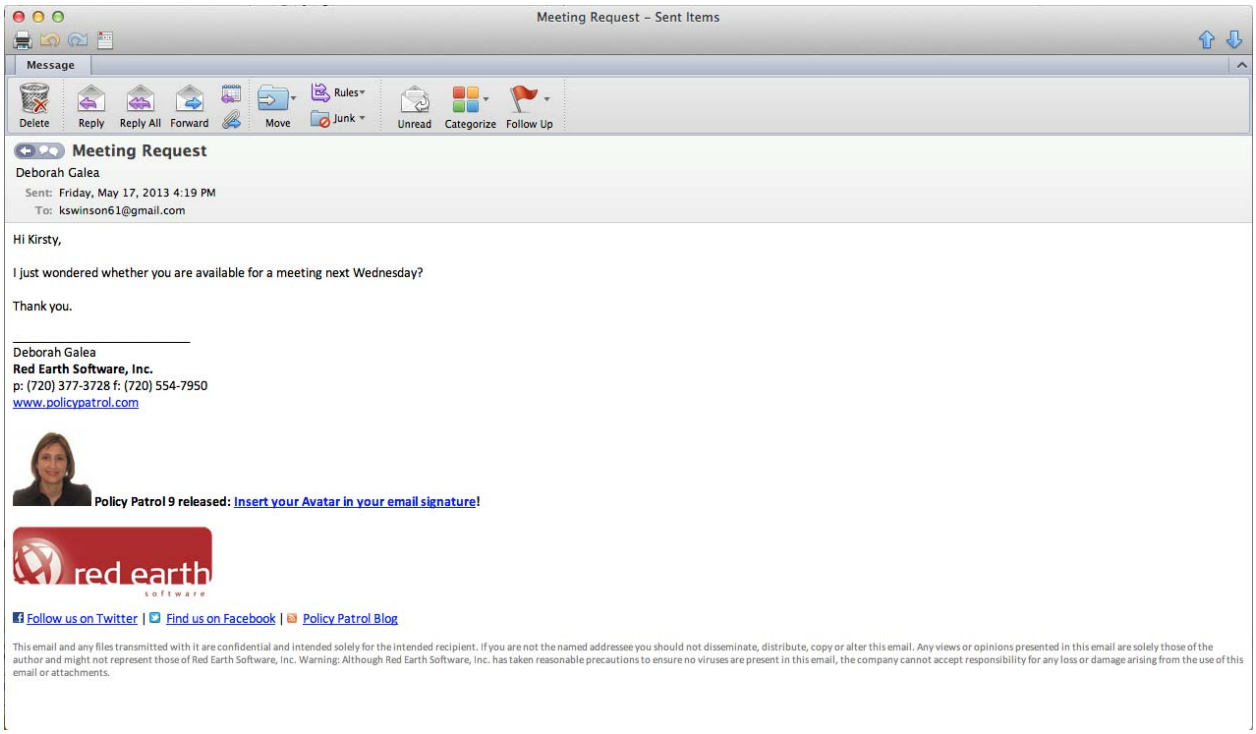
Policy Patrol allows you to automatically insert the sender's thumbnail picture into the email without having to upload and maintain your employees' pictures in Active Directory. Gravatar.com is a free service that stores a user's avatar (thumbnail picture) and then allows programs such as help desks 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)**.



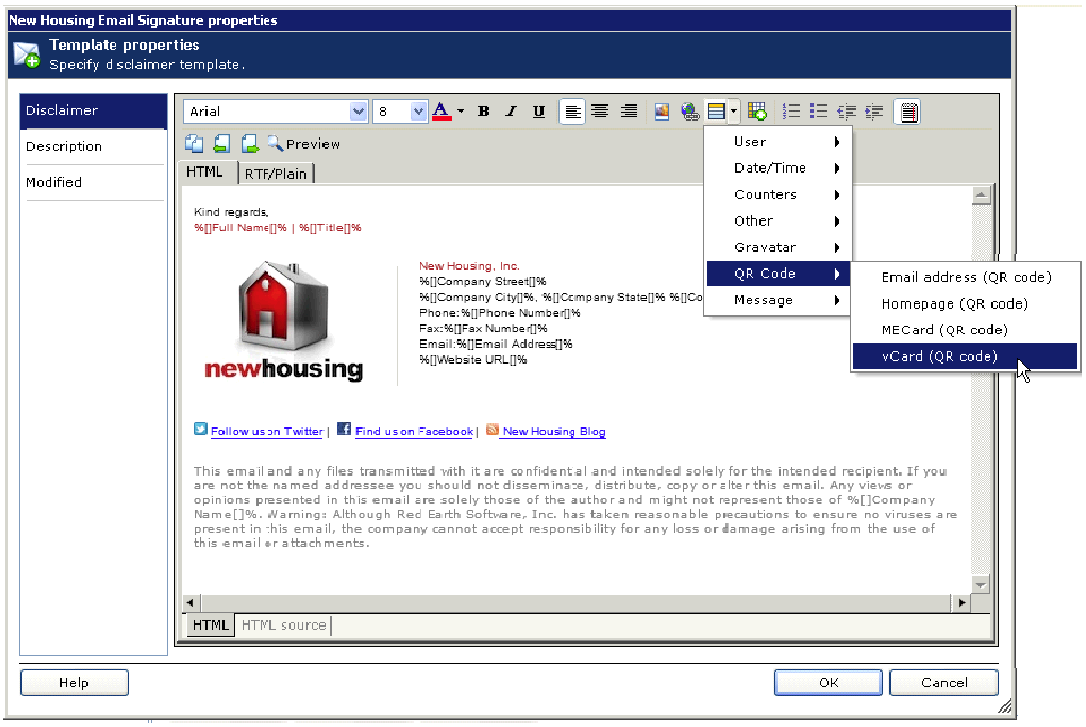
Below is a list of all Gravatar merge fields:

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



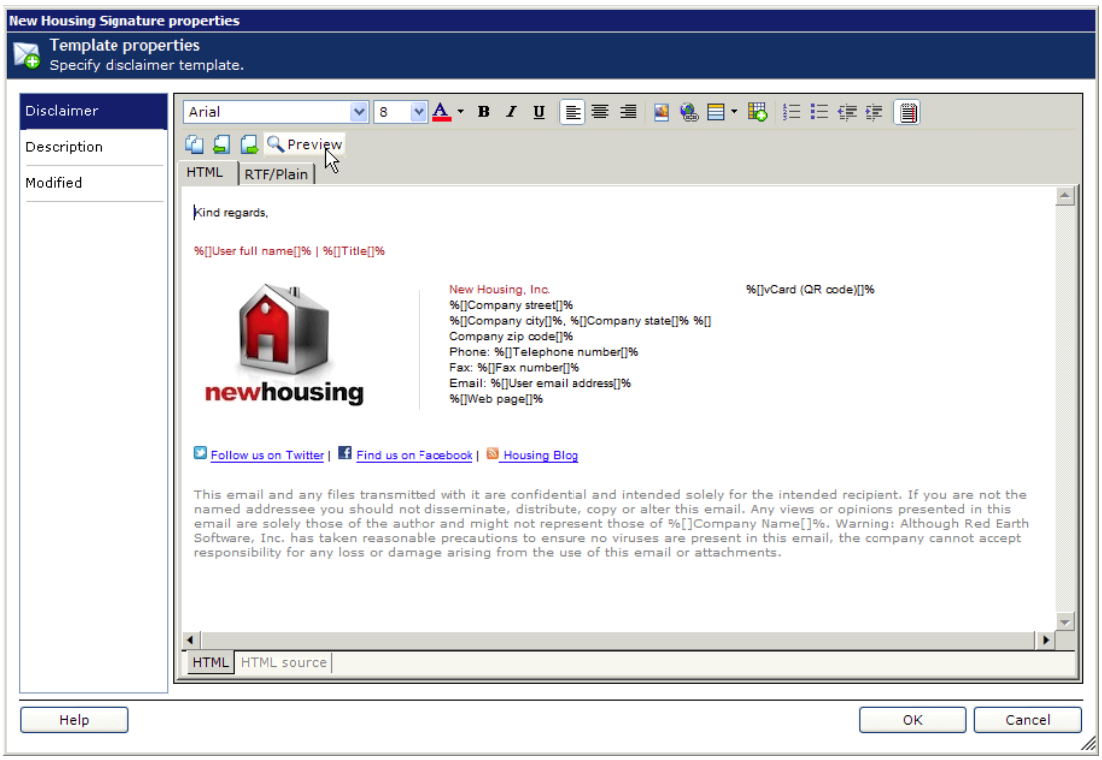
8.5 Inserting a QR Code in the Email Signature

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.

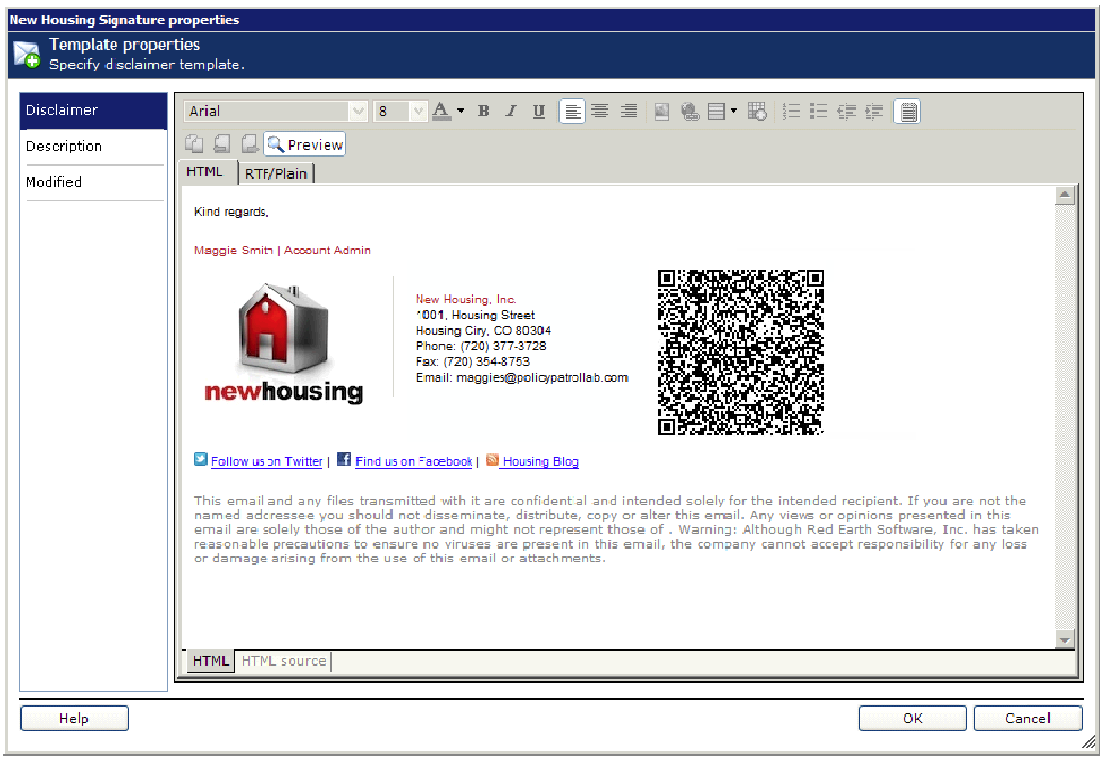


To insert the QR Code merge field into the email signature template, go to **Insert field**, select **QR Code** and the relevant field. Below is a list of the available QR codes:

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.



8.6 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.

8.6.1 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[]%">`.

8.6.2 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:)

8.7 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.

8.8 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>.

8.9 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.

8.10 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).

8.10.1 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.

8.10.2 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.

8.10.3 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

8.10.4 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.

8.11 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:

8.11.1.1 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.

8.11.1.2 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[]%`...

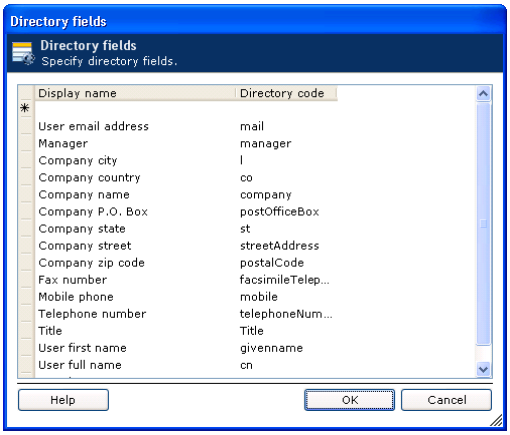
8.11.1.3 Specifying a Default Value if a Field Does not Exist

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.

8.12 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

9

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.

9.1 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.

9.1.1 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.



9.1.2 Email Threats Report

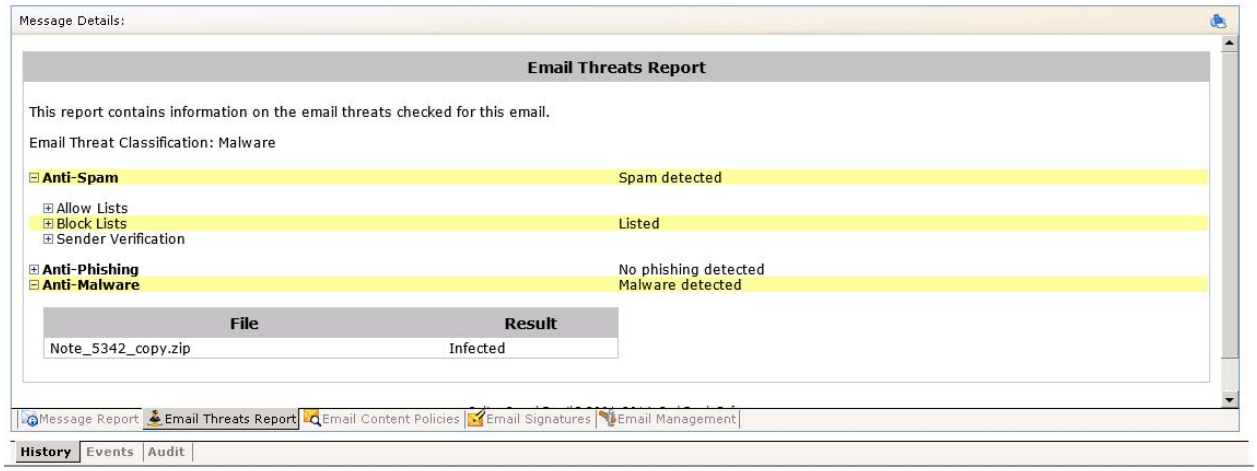
The Email Threats Report includes information on the results found for each email threat: Spam, Phishing and Malware. If a threat was found, the threat will be highlighted. Click on the plus signs to find the triggering event for the message. For instance for Anti-Spam, if the Block list is highlighted, 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.



9.1.3 Email Content Policies Report

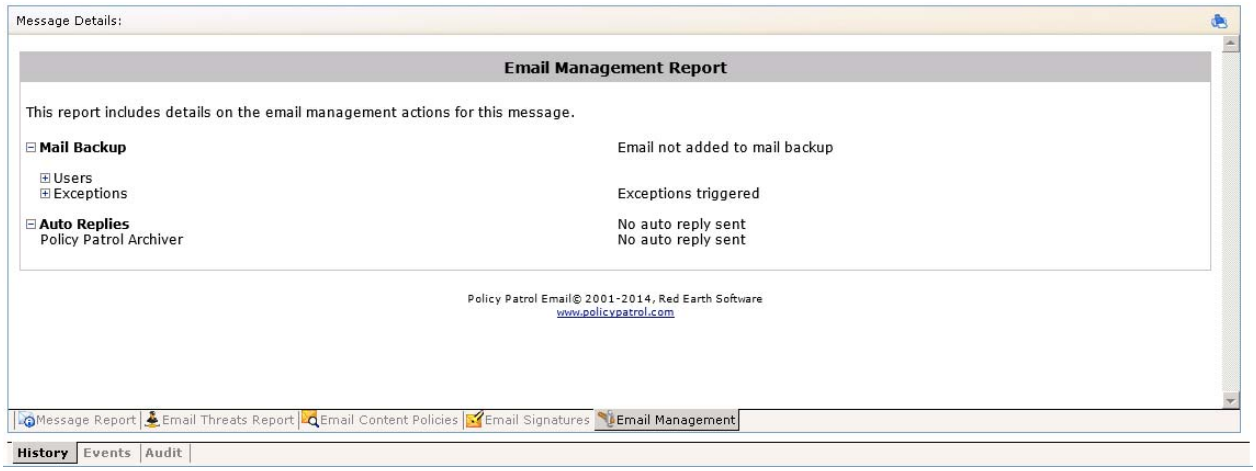
The Email Content Policies Report includes a list of all policies that were processed and whether they triggered for the message. Triggered policies will appear highlighted in the report. Each recipient will be listed separately, since different email policies can be applied for each recipient. To print the report, click on the **Print** icon in the top right hand corner.

9.1.4 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.

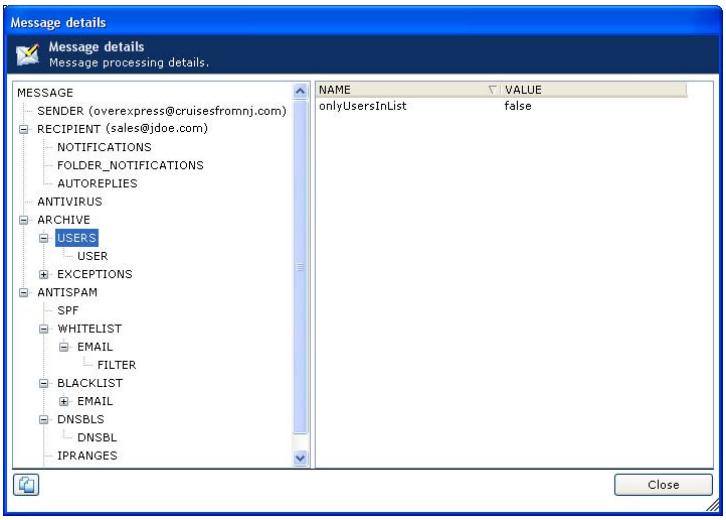
9.1.5 Email Management Report

The Email Management report will show whether the message was backed up and whether an auto reply was sent for the message.



9.1.6 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.



9.2 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.

9.3 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

10

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.

10.1 Auto Replies

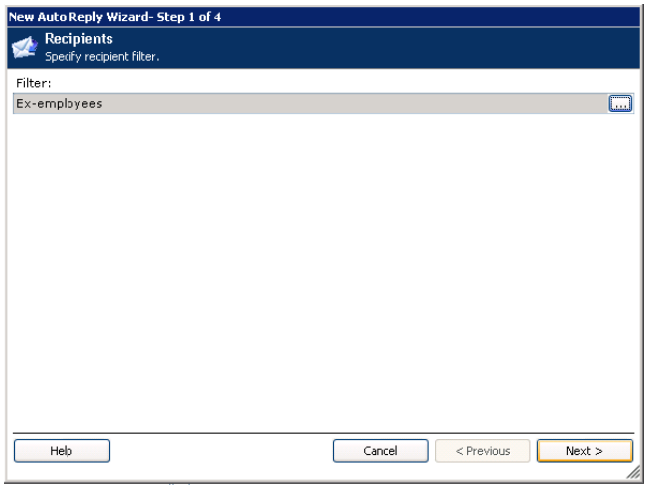
Policy Patrol includes the possibility to configure auto replies. This allows you to send auto replies to web forms and information requests, but also to send auto replies when messages are sent to email addresses of ex employees.

To configure a new auto reply:

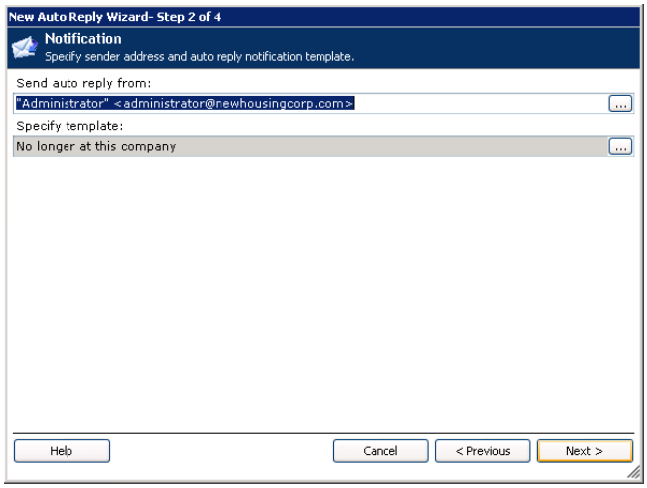
1. Go to **Email Management** > **Auto Replies**. Click **New**.

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

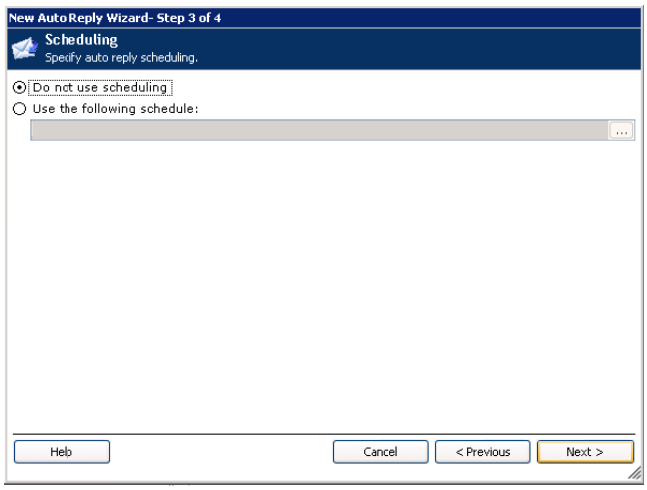
3. Select the recipient filter you wish to send the auto replies to by clicking on the **..** button. Select the filter from the list. If you wish to create a new filter, click on the **New** button above the available filters list. When you are done, click **OK**. Click **Next**.



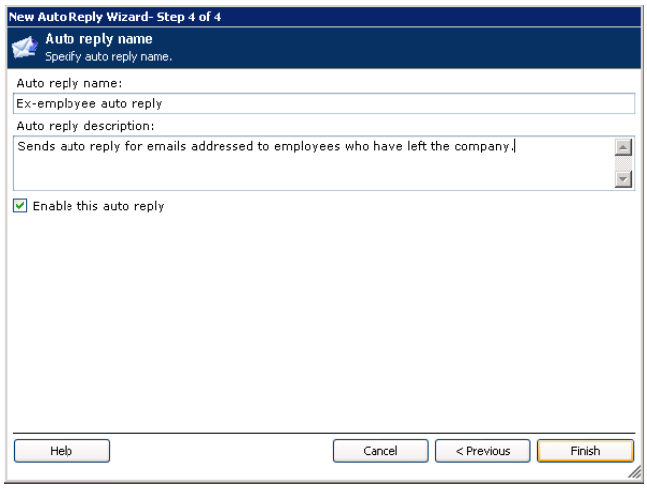
4. In 'Send auto reply from:' enter the email address to be included in the From address. Alternatively select a user by clicking on the **Browse** button. Now select the notification template to be used for the auto reply by clicking on the **..** button. Select the template from the list. If you wish 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**.

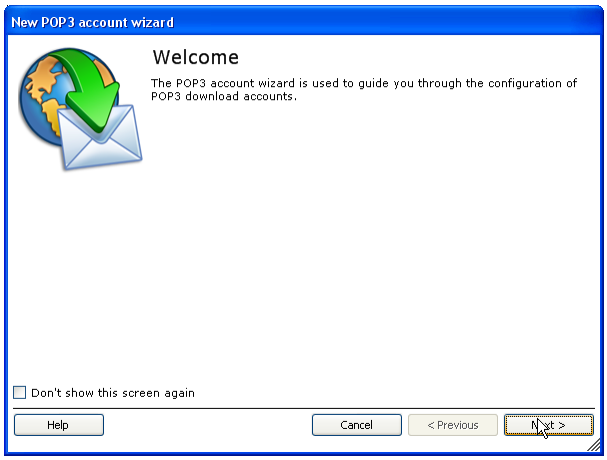
Tip

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.

10.2 POP3 Downloader

To create a new POP3 account to download messages from, follow the next steps:

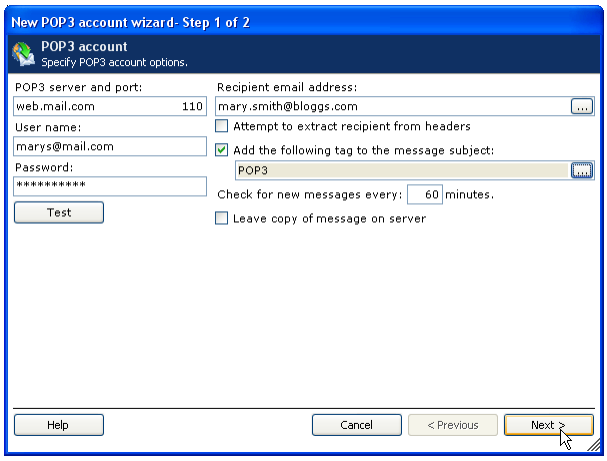
1. Go to **Email Management** > **POP3 Downloader** and click **New**.
2. In the Welcome screen, click **Next**.



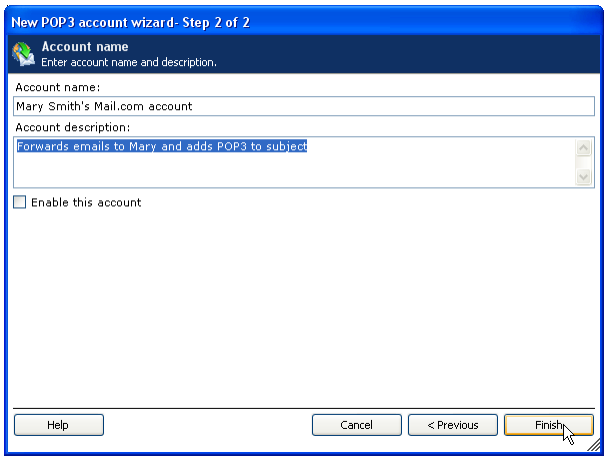
3. Enter the address of the POP3 server. Leave the Port at 110 unless you are using a different port. Enter the user name and password for the POP3 account. Click **Test** to verify the connection. Now specify to which email address the POP3 mails should be forwarded. If you wish to download email for 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

11

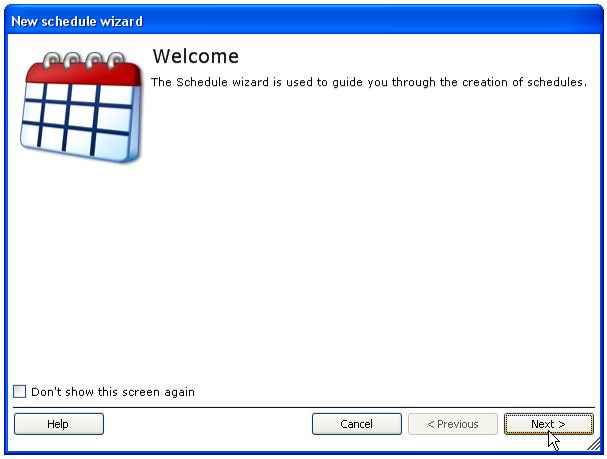
Settings

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.

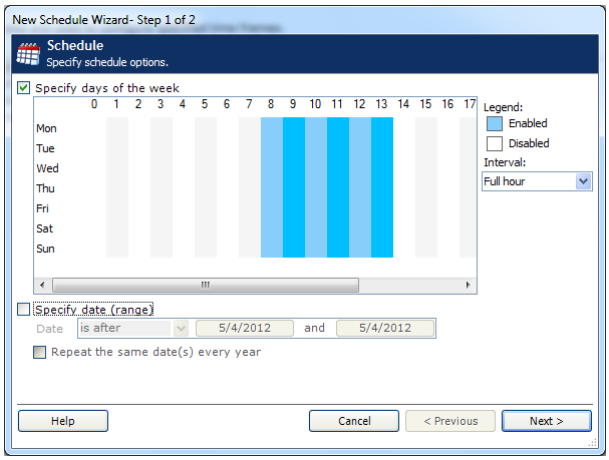
11.1 Schedules

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>.

11.2 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

12

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.

12.1 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.

12.2 Email Content Policies

This section lists the different configured policies and how often they have been applied in the selected time period.

12.3 Email Management

This section provides insight into the Email Management tools and how often they have triggered.

12.4 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.

12.5 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

13

Server Administration

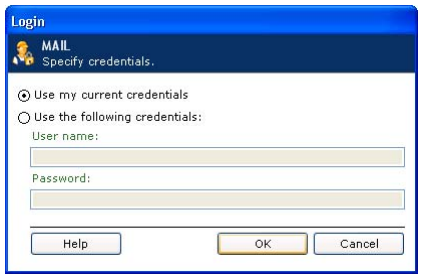
Policy Patrol includes some server options & settings that can be configured from the Policy Patrol server node(s), including user security, system configuration, system parameters, and automatic updates.

13.1 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.

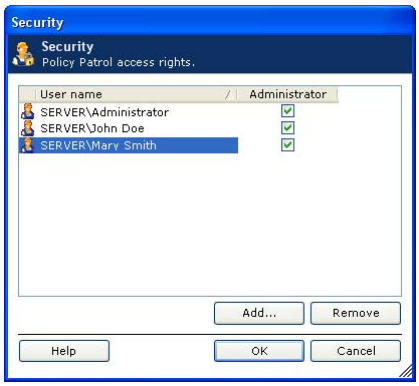
13.1.1 User Access Rights

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:

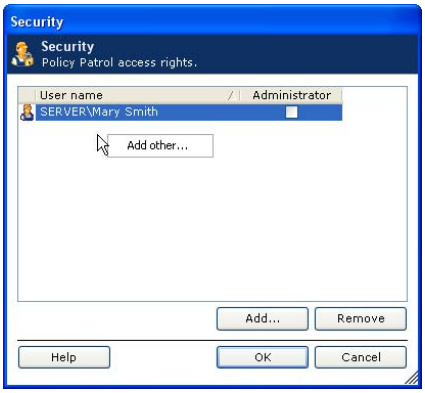
1. Select **<server name>**, expand **Security** and click on **User security**.



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.

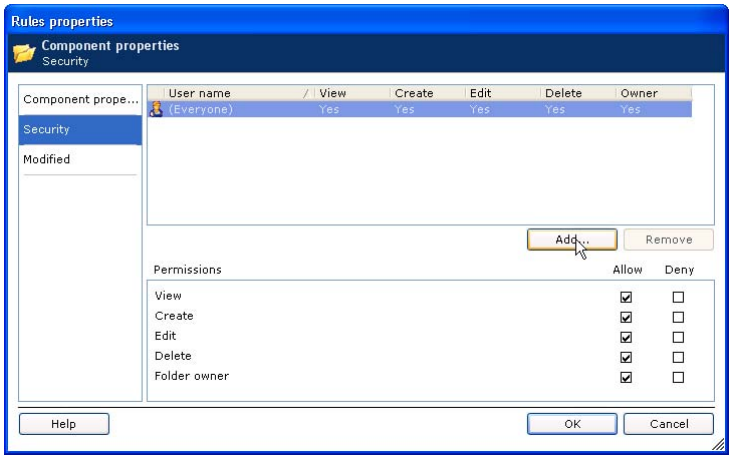
> **Note**
>
> If you wish to grant a user from another domain access rights, you can right-click in the Security list and select **Add other**. This will allow you to specify a user by entering the user name in DOMAIN\Username format.



13.1.2 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.

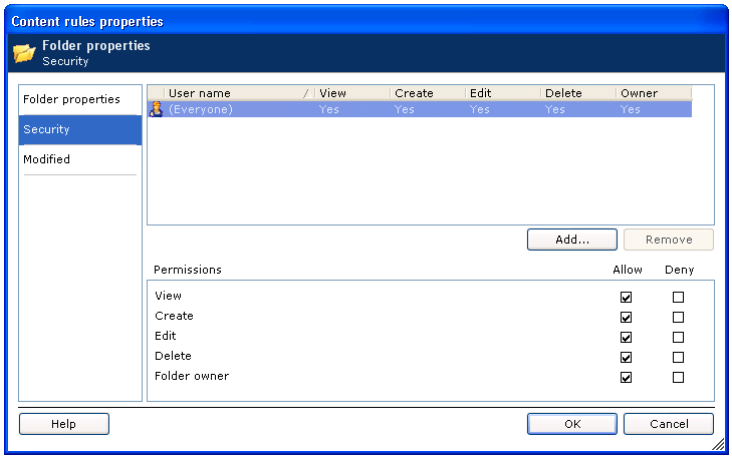
When you have finished editing permissions, click **OK**.

13.1.3 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.

13.1.4 Inheritance of Folder Rights

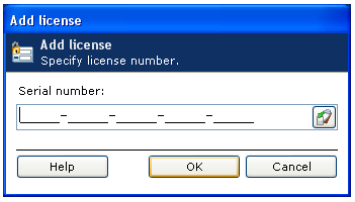
If you create a subfolder, the subfolder will inherit the permissions of the top folder. If you edit the rights for a folder that contains subfolders, the same changes will be applied to the subfolders.

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**..

13.2 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**.

13.3 System Configuration

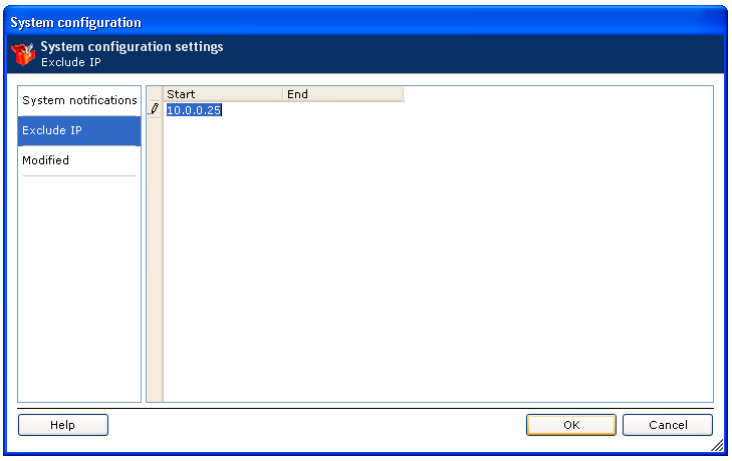
System configuration options are found in **<server name>** > **Advanced** > **System configuration**. The following tabs are available:

13.3.1 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.

13.3.2 Exclude IP

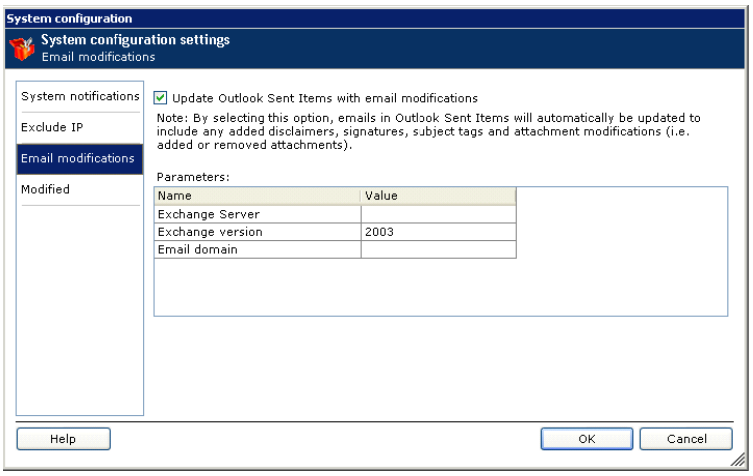
If you do not want Policy Patrol to process messages sent from a certain IP address, you can enter the IP address(es) in this Exclude IP list. To enter a single IP address, enter the IP address in **Start**. To enter an IP range, enter an IP address in **Start** and **End**.



13.3.3 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.

13.3.3.1 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.

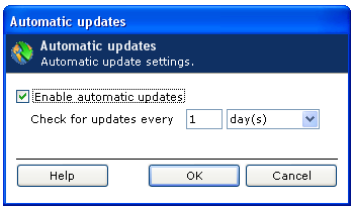
1. In 'Exchange version' your Exchange version should be entered (2007, 2010 or 2013).
2. In 'Exchange Server (CAS)' the name of your Exchange Client Access Server should be listed (even if this is the same machine as Policy Patrol is installed on). If you have multiple Exchange Servers, you need to 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.

13.4 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.

13.5 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**.



13.6 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**.

13.7 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**.

13.8 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.

13.8.1 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

13.8.2 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

13.9 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.

13.9.1 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

13.9.2 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

14

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.

14.1 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.

14.1.1 No Signatures are Being Added

If no signatures/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.

14.1.2 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.

14.1.3 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.

14.1.4 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.

14.1.5 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.

14.2 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/.

14.3 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 · 41
Active Directory · 84, 87, 88
Administrator address(es) · 108
Anti-virus · 54
Archive message · 35, 53, 66
Attachment exists · 40
Attachment name · 53, 58, 59
Attachment Name Filter · 59
Avatar · 77

B

Body · 35, 39
Bold · 66

C

Case sensitive · 55, 58, 59
Challenge/response · 87
Clustering · 7
Conditions · 35
Connector · 23, 26
Counter fields · 86

D

Date/Time fields · 86
Default value · 88
Delay message · 54
Delivery Status Notification · 36
Digitally signed · 36
Disclaimer · 41, 43, 46, 52, 53, 67, 68, 69, 73
Domain controller · 23
Domain/Email address filter · 60

E

Encrypted · 36
Exceptions · 34, 40, 53
Exchange 2000 · 6, 23
Exchange 2003 · 6
Exchange 2007 · 6, 12, 18, 23, 66
Exchange 2010 · 6, 23
Exchange 2013 · 6
Export · 58, 59, 60, 66, 71, 75
External messages · 85, 86

F

FAQs · 112
Field prefix · 87
Font color · 66
Font size · 66
Font type · 66
Frequently asked questions · 112

G

Gravatar · 77, 78

H

HTML source · 39
HTML stationery · 2, 100

I

Import · 58, 59, 60, 66, 71, 75
Inline attachments · 40
Insert Field · 63, 65, 69, 74
Insert image · 66, 71, 75
Installation · 10
Internal messages · 47, 86, 108
Italics · 66

K

Knowledge Base · 112

L

Lotus Notes · 7
Lotus Notes/Domino · 5, 7

M

Match all of the conditions · 35
Match any of the conditions · 35
meCard · 79, 80
Message fields · 85
Message priority · 36

Message sensitivity · 36
Microsoft .NET Framework · 5, 18

N

Non-inline attachments · 40
Notification message · 36, 63, 64, 66, 86

O

Ordering · 47, 53
Outlook Sent Items · 108

P

Permissions · 3, 104, 105, 106, 107
Plain text · 2, 64, 68, 69, 86
POP3 clients · 7
POP3 downloader · 97
Primary actions · 41
Process following rule(s) · 48

Q

QR Code · 79, 80
Quarantine message · 54
Quarantine remarks · 85

R

Regular Expression · 56, 57, 58
Remote administration · 18
Rename · 49, 62, 83
Replace words/phrases in subject · 46
RTF/plain text · 43, 68

S

Schedules · 100
Secondary actions · 41, 47, 53
Send blind copy · 47
Sender field contains domain or email address · 37
Subject · 35, 39, 53, 85
System parameters · 109
System requirements · 5

T

Tag · 39, 53, 67
Tag template · 66
Templates · 63, 67, 83
Thumbnail picture · 77
Tracking numbers · 86

U

Underline · 66
User fields · 84, 88
Users · 7, 23, 26, 34, 53

V

Virus · 85

W

Whole or part of word(s) are matched · 57, 58
Whole word(s) are matched · 57, 58
Word score · 57, 58
Word/Phrase filter · 55