

# Exclaimer Mail Utilities Manual



**Exclaimer**  
UK +44 (0) 845 050 2300  
USA 1-888-450-9631  
[info@exclaimer.com](mailto:info@exclaimer.com)

# Copyright Notice

The information in this document is subject to change without notice. Exclaimer Ltd assumes no responsibility for any errors that may appear in this document. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious and not associated with any real company, organization, product, domain name, e-mail address, logo, person, place or event.

Exclaimer Mail Utilities and other Exclaimer devices are either registered trademarks or trademarks of Exclaimer Ltd in the United Kingdom and/or other countries. Exclaimer may have trademarks, copyrights or other intellectual property rights covering subject matter in this document. All other company and product names are acknowledged as being the trademarks or registered trademarks of their respective companies.

Unless expressly provided in a written license agreement from Exclaimer Ltd, the furnishing of this document does not give you any license to these trademarks, copyrights or other intellectual property.

Copyright 2008, Exclaimer Ltd. All rights reserved. This document may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without the express written permission of Exclaimer Ltd. Complying with all applicable copyright laws is the responsibility of the user.

# Revision History

| Date                            | Revision                  |
|---------------------------------|---------------------------|
| 20 <sup>th</sup> February 2007  | Initial Publication       |
| 23 <sup>rd</sup> April 2007     | Post Internal Review      |
| 17 <sup>th</sup> August 2007    | 4.31 additions and amends |
| 26 <sup>th</sup> September 2007 | 4.50 + 2007 updates       |
| 15 <sup>th</sup> January 2008   | Copyright update          |

**First Published** 20<sup>th</sup> February 2007

**Author** Ben Gower

**Editor(s)** Gary Levell

**Reviewer(s)** Chris Crawshay

# Table of Contents

|  |            |
|--|------------|
| <b>Introduction</b> .....  | <b>4</b>   |
| <b>Who should read this manual</b> .....                                 | <b>4</b>   |
| <b>System requirements</b> .....   | <b>5</b>   |
| Server requirements .....  | 5          |
| <b>Chapter 1</b> .....   | <b>6</b>   |
| <b>Installing and configuring Exclaimer Mail Utilities</b> .....         | <b>6</b>   |
| <b>Installing Exclaimer Mail Utilities</b> .....                         | <b>6</b>   |
| To install Exclaimer Mail Utilities .....                                | 6          |
| <b>The Setup Wizard</b> .....  | <b>10</b>  |
| To configure Exclaimer Mail Utilities using the Setup Wizard.....        | 10         |
| <b>The Auto-Whitelist Wizard</b> .....                                   | <b>24</b>  |
| To configure the Auto-Whitelist using the Auto-Whitelisting Wizard ..... | 24         |
| <b>Chapter 2</b> .....   | <b>27</b>  |
| <b>Exclaimer Mail Utilities – The Control Panel</b> .....                | <b>27</b>  |
| <b>Main menu</b> .....   | <b>27</b>  |
| The Main menu .....  | 27         |
| <b>Setup panel</b> .....   | <b>29</b>  |
| The Setup panel .....  | 29         |
| <b>Remote Deployment</b> .....   | <b>33</b>  |
| The Remote Deployment box .....  | 33         |
| To set up Remote Deployment .....  | 34         |
| To set up a shared folder .....  | 35         |
| Deploy settings to slave mail servers .....                              | 35         |
| <b>Passwords</b> .....   | <b>37</b>  |
| The Set Password box .....   | 37         |
| <b>Advanced Settings</b> .....   | <b>38</b>  |
| The Advanced Settings box .....  | 38         |
| <b>Default Rules panel</b> .....   | <b>49</b>  |
| The Default Rules panel.....   | 49         |
| <b>Custom Rules panel</b> .....  | <b>53</b>  |
| The Custom Rules panel .....   | 53         |
| <b>Add Mail Rule box</b> .....   | <b>55</b>  |
| The Add Mail Rule box .....  | 55         |
| <b>Rule Tester panel</b> .....   | <b>66</b>  |
| The Rule Tester panel .....  | 66         |
| <b>Anti-Spam Settings panel</b> .....                                    | <b>69</b>  |
| The Anti-Spam Settings panel .....                                       | 69         |
| <b>Anti-Virus Settings panel</b> .....                                   | <b>81</b>  |
| The Anti-Virus Settings panel .....                                      | 81         |
| <b>Logging &amp; Stats panel</b> .....                                   | <b>83</b>  |
| The Logging & Statistics panel.....                                      | 83         |
| <b>About panel</b> .....   | <b>94</b>  |
| The About panel .....  | 94         |
| Applying a license.....  | 95         |
| <b>Appendix A</b> .....  | <b>96</b>  |
| <b>Exclaimer Mail Utilities – Other tools and features</b> .....         | <b>96</b>  |
| <b>Disclaimer Editor</b> .....   | <b>97</b>  |
| The Disclaimer Editor box .....  | 97         |
| <b>Disclaimer Options</b> .....  | <b>109</b> |
| The Disclaimer Options box.....  | 109        |
| <b>Templates</b> .....   | <b>110</b> |
| The Template Manager box .....   | 110        |
| The Insert Template box.....   | 111        |
| <b>User Defined Fields</b> .....   | <b>113</b> |
| The User Defined Fields box .....  | 113        |
| The Insert User Defined Fields box.....                                  | 115        |

**Active Directory Attribute Query Editor .....116**  
The Active Directory Attribute Query Editor box..... 116

**Index ..... 120**

# Introduction

The *Exclaimer Mail Utilities Manual* is designed to help you become familiar with the set up process and Exclaimer Mail Utilities' Control Panel.

## Who should read this manual

This guide is designed to benefit the following professionals:

### Mail Utilities Trial Users

Those individuals who are evaluating our mail utilities software and who wish to start evaluating the software as soon as possible

### People who have purchased without trial

Organizations that have purchased the software on recommendation without having a trial period.

### SBS users

Individuals or Organizations who utilize Microsoft SBS server.

#### **IMPORTANT!**

*This manual contains technical terms and concepts that some people may be unfamiliar with. We have done our best to ensure that all technical terms and concepts are explained as clearly and concisely as possible. However, if you are having problems understanding any elements of this manual we recommend that you consult a Microsoft Exchange or email professional.*

*Alternatively, you could also contact Exclaimer Technical Support at [support@exclaimer.com](mailto:support@exclaimer.com) for assistance and advice.*

## System requirements

Prior to installation of the Exclaimer Mail Utilities software, please ensure that you have the following resources available.

For Exclaimer Mail Utilities' system requirements go to <http://www.exclaimer.com/MailUtilities-SystemRequirements.aspx>

### Server requirements

- A Microsoft Windows Active Directory network.
- A Microsoft Windows server with Active Directory and the Microsoft SMTP Service or a Microsoft Windows Server with Exchange.
- Exclaimer Mail Utilities must be installed on the server that routes your organization's email.
- If you are installing Exclaimer Mail Utilities 2007 you must have an Exchange 2007 server.

# Chapter 1

## Installing and configuring Exclaimer Mail Utilities

This chapter describes how to install Exclaimer Mail Utilities and configure it. Please ensure that you have the required system environment as detailed in the Introduction.

### ▶ Installing Exclaimer Mail Utilities

#### IMPORTANT!

Before installing Exclaimer Mail Utilities check that you have the latest version by visiting our website and downloading it.

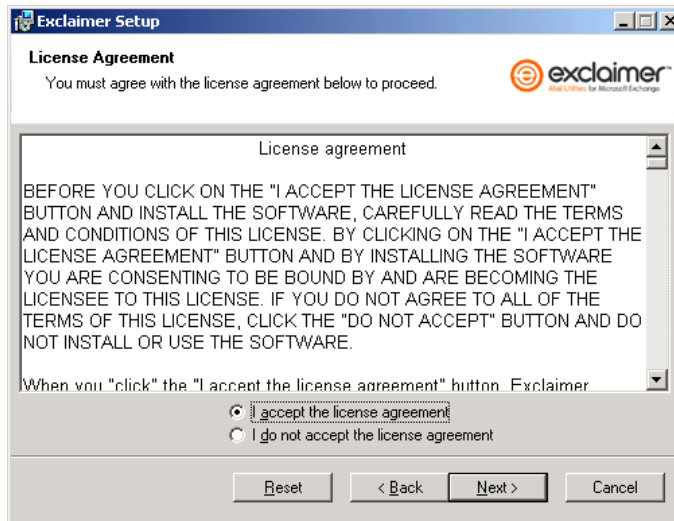
#### To install Exclaimer Mail Utilities

1. Log on as an Enterprise Administrator to the server where you intend to install Exclaimer Mail Utilities.
2. Double click the Exclaimer.exe file.
3. Click on **Next >**.

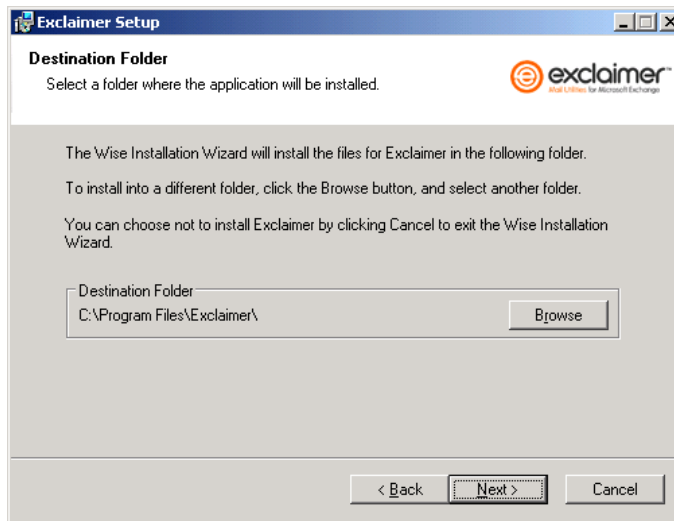


4. Read the Exclaimer Mail Utilities license agreement. If you agree to the terms select the **I accept the license agreement** radio button.

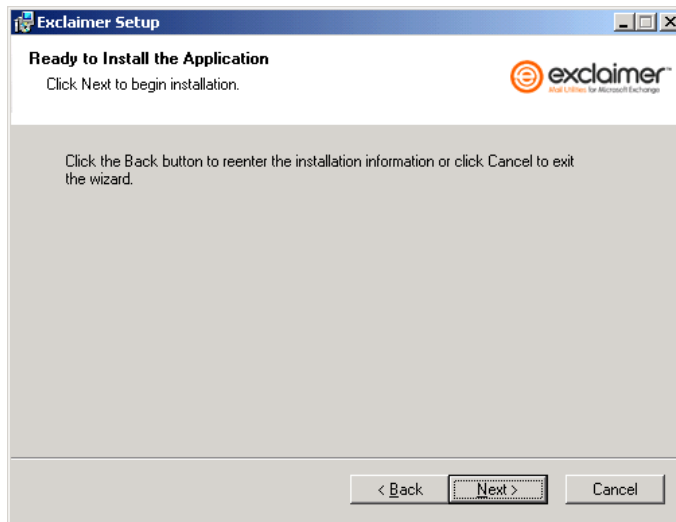
Click on **Next >**.



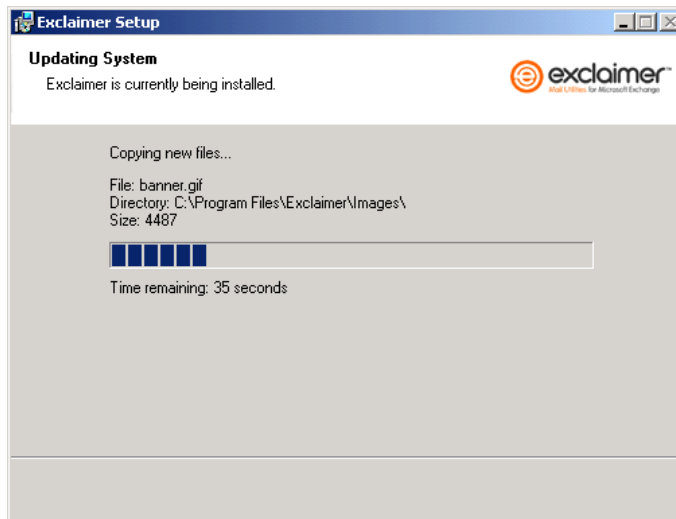
5. This is where you can select the folder that you want to install Mail Utilities in. Click on the **Browse** button to change the default folder location or click on **Next >** to use the default location.



- To begin the installation click on **Next >**.



- Exclaimer Mail Utilities will be installed on your server.



- To complete the installation click on **Finish**.



**NOTE**

*You do not have to stop or restart any services when you install Exclaimer Mail Utilities.*

Congratulations, you have successfully installed Exclaimer Mail Utilities. You now need to configure the Mail Utilities software. Details of how to perform this operation are covered next in *The Setup Wizard* section.

## ▶ The Setup Wizard

This section describes how to navigate the Mail Utilities Setup Wizard.

The Exclaimer Mail Utilities Setup Wizard should have started automatically after you finished the installation.

Please note that Exclaimer Mail Utilities will not start processing any email until the Setup Wizard is complete.

### To configure Exclaimer Mail Utilities using the Setup Wizard

1. The wizard should start. Click on **Next >**.



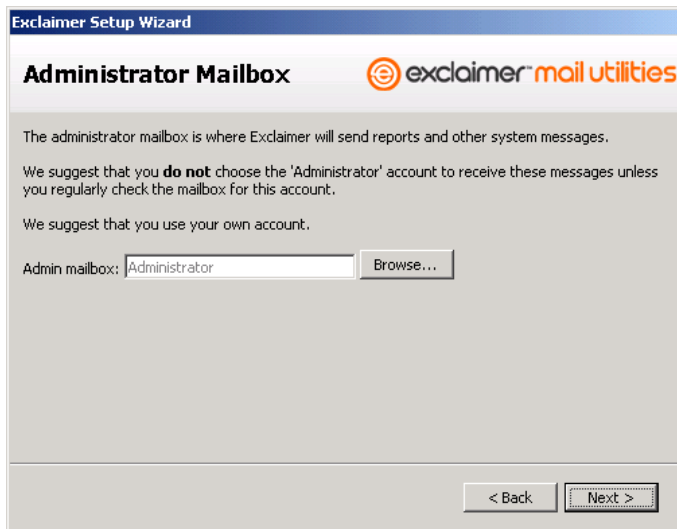
2. Select the account that you want Exclaimer Mail Utilities to send reports and other system messages to.

**WARNING!**

*We do not recommend that you use the Administrator account. It is best to set up a different account specifically for Exclaimer Mail Utilities' reports and other system messages.*

*This should be an account that you access regularly to ensure that important Exclaimer Mail Utilities reports and messages are not missed. We recommend that you use your own email account or that of your organization's email administrator.*

Click on **Next >**.

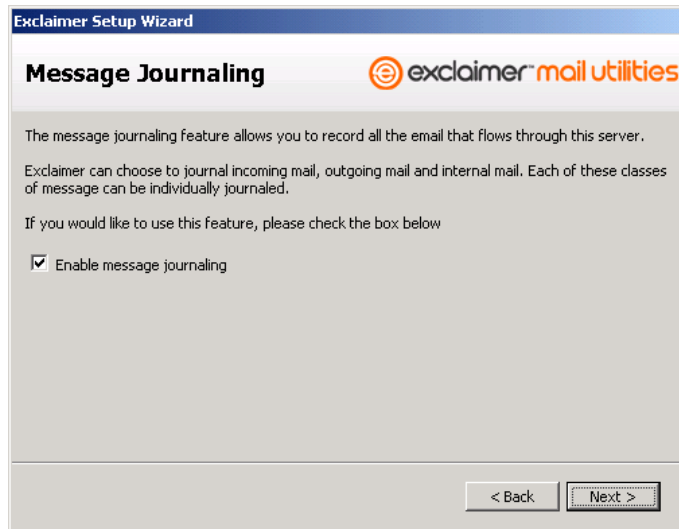


The screenshot shows a window titled "Exclaimer Setup Wizard" with the "Administrator Mailbox" section. The Exclaimer Mail Utilities logo is in the top right. The text explains that the administrator mailbox is for reports and system messages, and advises against using the 'Administrator' account unless regularly checked. It suggests using a personal or organizational account. Below this is a text input field containing "Administrator" and a "Browse..." button. At the bottom right are "< Back" and "Next >" buttons.

3. You can use the message journaling feature to BCC a mailbox into of all your organization's email messages (incoming, internal and outgoing).

Enable the **Enable message journaling** checkbox if you want to activate Exclaimer Mail Utilities' message journaling capabilities.

Click on **Next >**.

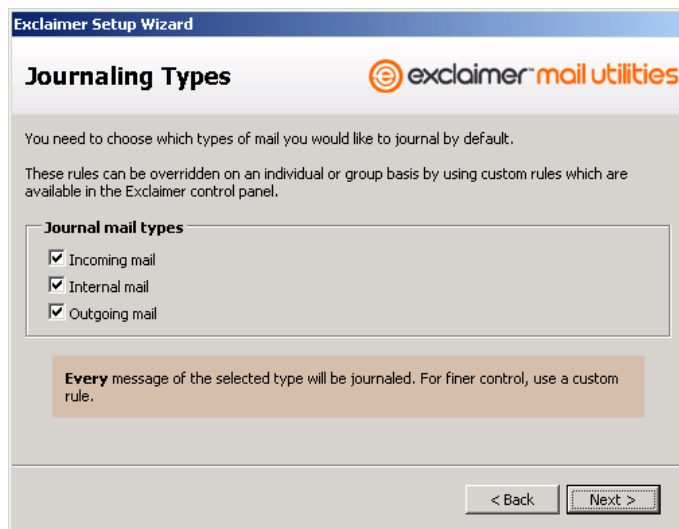


The screenshot shows the 'Exclaimer Setup Wizard' window. The title bar reads 'Exclaimer Setup Wizard'. The main heading is 'Message Journaling' with the Exclaimer Mail Utilities logo to its right. Below the heading, there is explanatory text: 'The message journaling feature allows you to record all the email that flows through this server. Exclaimer can choose to journal incoming mail, outgoing mail and internal mail. Each of these classes of message can be individually journaled. If you would like to use this feature, please check the box below'. A checkbox labeled 'Enable message journaling' is checked. At the bottom right, there are two buttons: '< Back' and 'Next >'.

4. This step in the wizard only appears if you have enabled message journaling.

Enable the options that correspond to the type of email messages you want to journal.

Click on **Next >**.



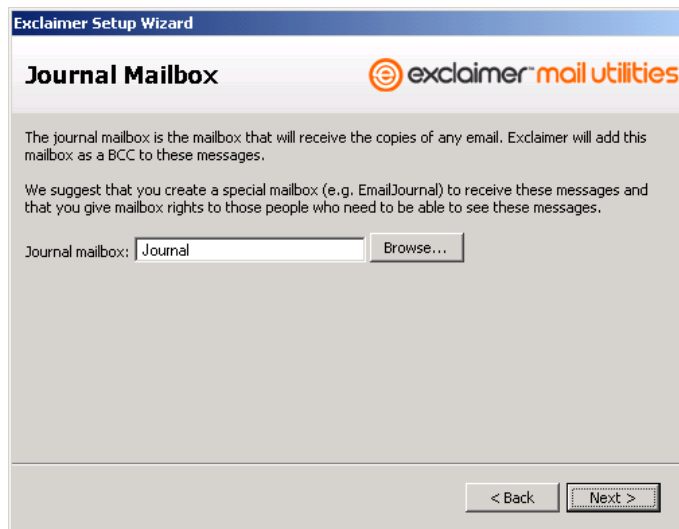
The screenshot shows the 'Exclaimer Setup Wizard' window. The title bar reads 'Exclaimer Setup Wizard'. The main heading is 'Journaling Types' with the Exclaimer Mail Utilities logo to its right. Below the heading, there is explanatory text: 'You need to choose which types of mail you would like to journal by default. These rules can be overridden on an individual or group basis by using custom rules which are available in the Exclaimer control panel.' A section titled 'Journal mail types' contains three checked checkboxes: 'Incoming mail', 'Internal mail', and 'Outgoing mail'. Below this section, a light brown box contains the text: 'Every message of the selected type will be journaled. For finer control, use a custom rule.' At the bottom right, there are two buttons: '< Back' and 'Next >'.

5. This step in the wizard only appears if you have enabled message journaling.

Select the mailbox that you want to receive the journaled email.

The email is BCC'd as it is received at the server so that neither the sender nor the recipient/s will know that it has been journaled.

Click on **Next >**.



The screenshot shows the 'Exclaimer Setup Wizard' window. The title bar reads 'Exclaimer Setup Wizard'. The main heading is 'Journal Mailbox' with the Exclaimer Mail Utilities logo to its right. Below the heading, there is explanatory text: 'The journal mailbox is the mailbox that will receive the copies of any email. Exclaimer will add this mailbox as a BCC to these messages.' and 'We suggest that you create a special mailbox (e.g. EmailJournal) to receive these messages and that you give mailbox rights to those people who need to be able to see these messages.' Below this text is a text input field labeled 'Journal mailbox:' containing the text 'Journal', and a 'Browse...' button to its right. At the bottom of the window are '< Back' and 'Next >' buttons.

6. Enable the **Enable Anti-Spam filter** checkbox if you want to activate Exclaimer Mail Utilities' Anti-Spam filter.

Click on **Next >**.

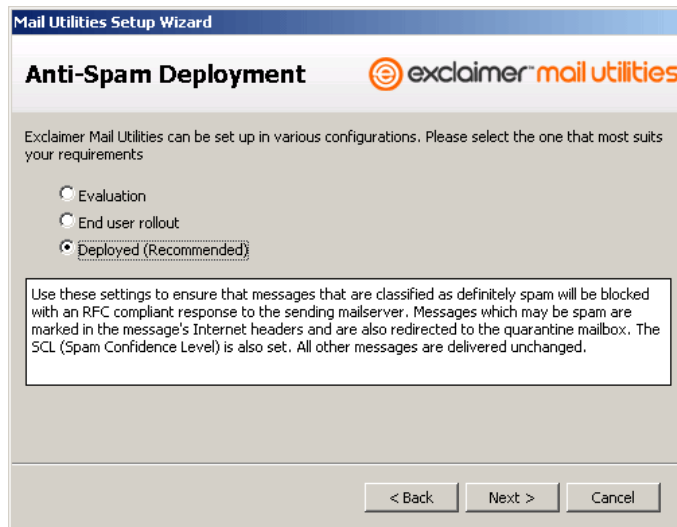


The screenshot shows the 'Exclaimer Setup Wizard' window. The title bar reads 'Exclaimer Setup Wizard'. The main heading is 'Anti-Spam Filter' with the Exclaimer Mail Utilities logo to its right. Below the heading, there is explanatory text: 'Exclaimer's anti-spam technology allows you to filter out unsolicited incoming bulk or spam emails.' and 'If you would like to use this feature, please check the box below'. Below this text is a checkbox labeled 'Enable Anti-Spam filter' which is checked. At the bottom of the window are '< Back' and 'Next >' buttons.

7. This step in the wizard only appears if you have enabled Anti-Spam filter.

Select the option that corresponds to the type of Anti-Spam deployment you want to use.

Click on **Next >**.



The screenshot shows a window titled "Mail Utilities Setup Wizard" with a sub-header "Anti-Spam Deployment" and the Exclaimer Mail Utilities logo. The main text reads: "Exclaimer Mail Utilities can be set up in various configurations. Please select the one that most suits your requirements". There are three radio button options: "Evaluation", "End user rollout", and "Deployed (Recommended)". The "Deployed (Recommended)" option is selected. Below the options is a text box containing the following text: "Use these settings to ensure that messages that are classified as definitely spam will be blocked with an RFC compliant response to the sending mailserv. Messages which may be spam are marked in the message's Internet headers and are also redirected to the quarantine mailbox. The SCL (Spam Confidence Level) is also set. All other messages are delivered unchanged." At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

**IMPORTANT!**

*If you have upgraded or reinstalled Exclaimer Mail Utilities your settings will be preserved. However, if you have deleted the folder where the previous version of Exclaimer Mail Utilities was installed or you have changed the location of the installation folder your settings will not be preserved.*

8. Enable the **Enable Anti-Virus Protection** checkbox if you want to activate Exclaimer Mail Utilities' Anti-Virus protection.

Click on **Next >**.

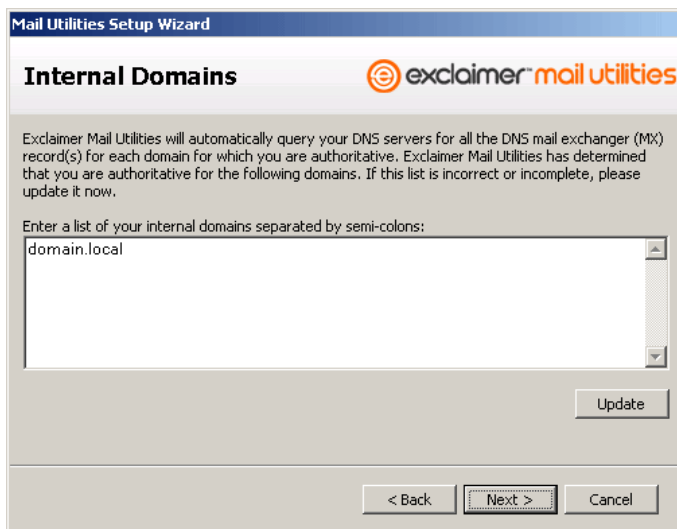


9. Select all the domains that you are authoritative for that you want Exclaimer Mail Utilities to work with.

**IMPORTANT!**

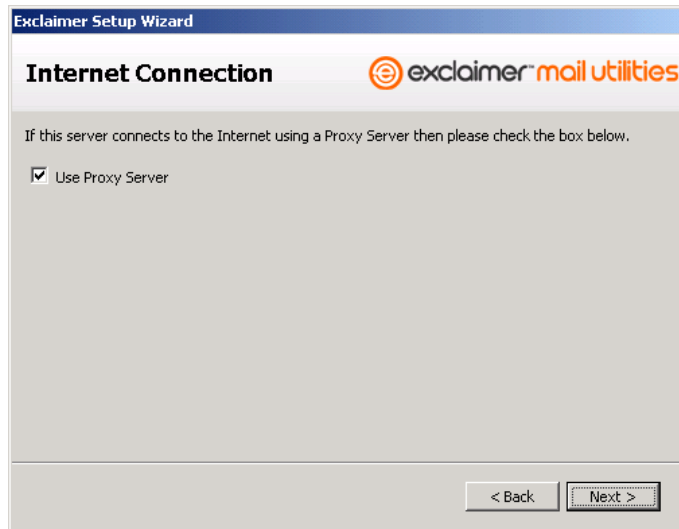
*If you are upgrading click on the **Update** button to ensure Exclaimer Mail Utilities checks for the most up-to-date list of domains you are authoritative for.*

Click on **Next >**.



10. Enable the **Use Proxy Server** checkbox if your server connects to the Internet using a Proxy Server.

Click on **Next >**.

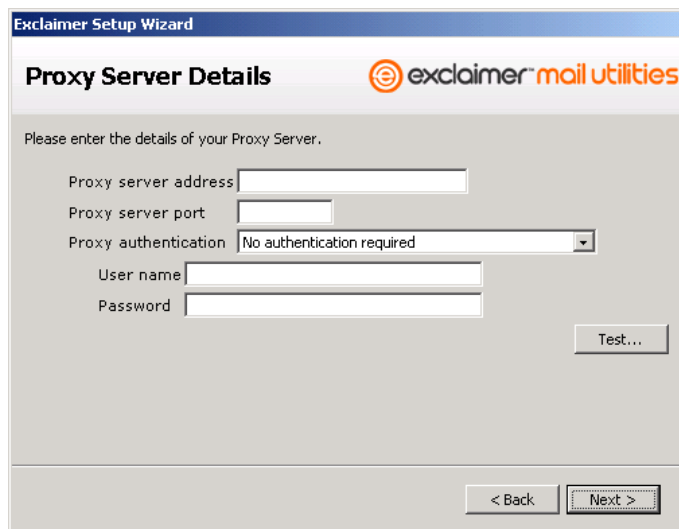


The screenshot shows the 'Exclaimer Setup Wizard' window with the title 'Internet Connection'. The 'exclaimer mail utilities' logo is in the top right. Below the title, it says 'If this server connects to the Internet using a Proxy Server then please check the box below.' There is a checked checkbox labeled 'Use Proxy Server'. At the bottom right, there are '< Back' and 'Next >' buttons.

11. This step in the wizard only appears if you placed a tick in the **Use Proxy Server** checkbox in the previous step.

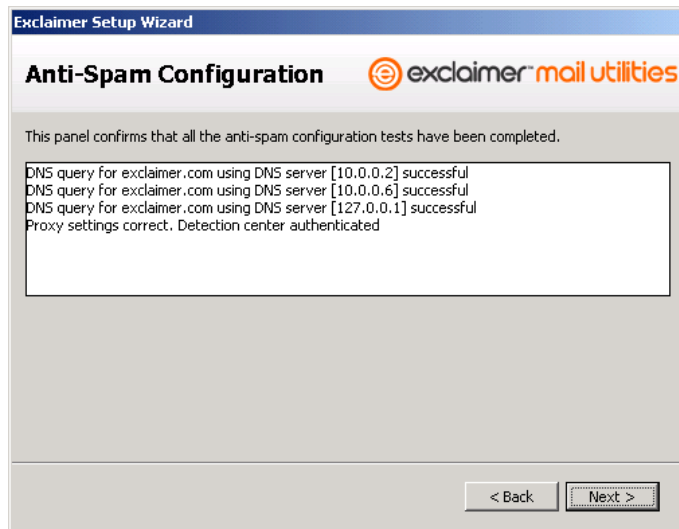
Fill out your Proxy Server details and test the connection.

Click on **Next >**.



The screenshot shows the 'Exclaimer Setup Wizard' window with the title 'Proxy Server Details'. The 'exclaimer mail utilities' logo is in the top right. Below the title, it says 'Please enter the details of your Proxy Server.' There are four input fields: 'Proxy server address', 'Proxy server port', 'User name', and 'Password'. The 'Proxy authentication' dropdown menu is set to 'No authentication required'. A 'Test...' button is located to the right of the input fields. At the bottom right, there are '< Back' and 'Next >' buttons.

- Click on **Next >**.



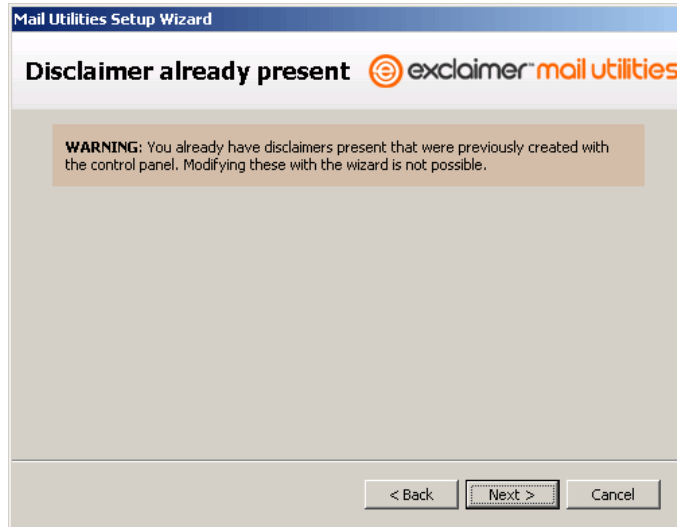
- Enable the **Enable Disclaimers** checkbox if you want to add disclaimers to your email messages.

Click on **Next >**.



This step in the wizard only appears if you are upgrading from a previous version of Exclaimer Mail Utilities and have had disclaimers already set up.

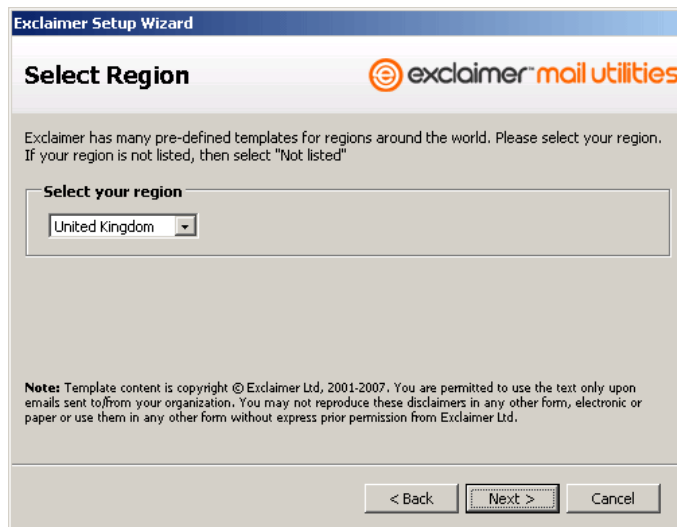
Click on **Next >** to move to the Wizard Complete page and finish the Setup Wizard.



14. This step in the wizard only appears if you have enabled disclaimers and you are installing as a brand new installation of Exclaimer Mail Utilities.

Select your region from the **Select your region** drop down list.

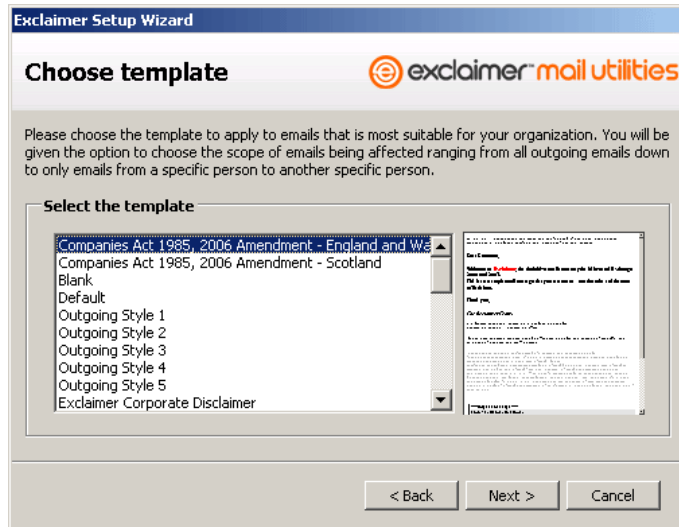
Click on **Next >**.



15. This step in the wizard only appears if you have enabled disclaimers.

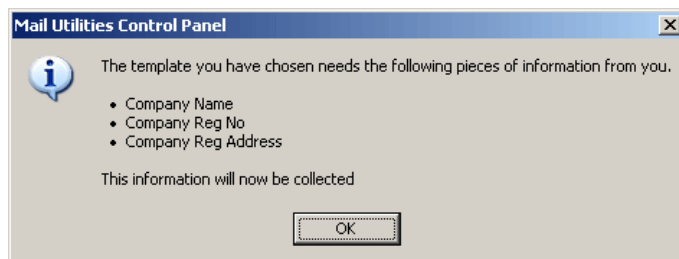
Select the disclaimer that you want to appear on your outgoing email.

Click on **Next** > .



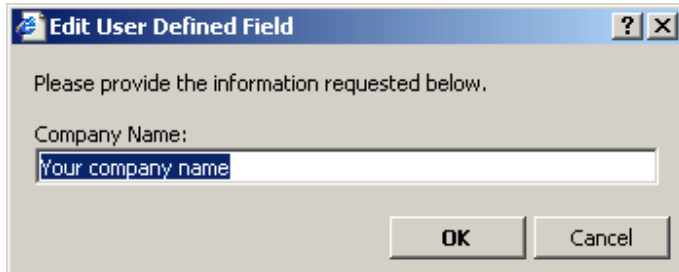
16. This step in the wizard only appears if you have selected a disclaimer that requires User Defined Fields.

If you select a template that requires User Defined Fields you will be informed then asked for the information needed. Click on **OK** and fill out the required fields.



17. These steps in the wizard only appear if you have selected a disclaimer that requires User Defined Fields.

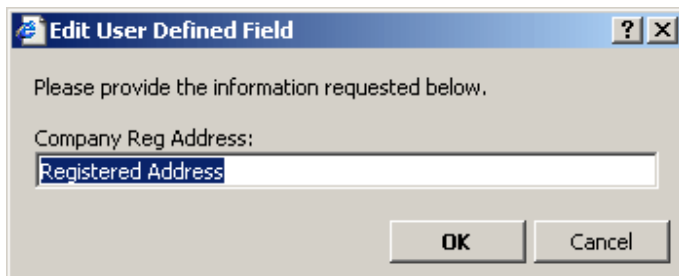
Enter the requested information into each of the boxes that appear and click on **OK**.



The screenshot shows a dialog box titled "Edit User Defined Field" with a question mark icon and a close button. The text inside reads "Please provide the information requested below." Below this is a label "Company Name:" followed by a text input field containing the placeholder text "Your company name". At the bottom right are two buttons: "OK" and "Cancel".



The screenshot shows a dialog box titled "Edit User Defined Field" with a question mark icon and a close button. The text inside reads "Please provide the information requested below." Below this is a label "Company Reg No:" followed by a text input field containing the placeholder text "Registration No". At the bottom right are two buttons: "OK" and "Cancel".

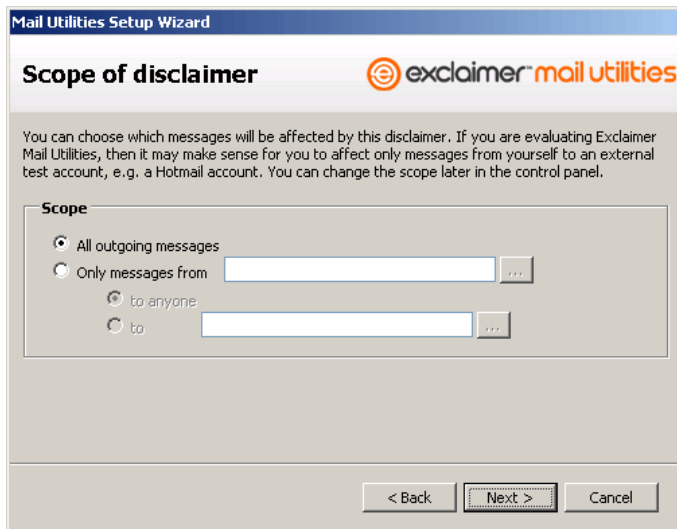


The screenshot shows a dialog box titled "Edit User Defined Field" with a question mark icon and a close button. The text inside reads "Please provide the information requested below." Below this is a label "Company Reg Address:" followed by a text input field containing the placeholder text "Registered Address". At the bottom right are two buttons: "OK" and "Cancel".

18. This step in the wizard only appears if you have enabled disclaimers.

This is where you can set up your disclaimer so that it is either added to all outgoing messages or to messages sent from a particular email address/user. This can be useful to ensure that your disclaimer looks and works in the way you want before you roll it out to cover all your outgoing email.

Click on **Next >**.



The screenshot shows a window titled "Mail Utilities Setup Wizard" with the "exclaimer mail utilities" logo. The main heading is "Scope of disclaimer". Below the heading is a paragraph of text: "You can choose which messages will be affected by this disclaimer. If you are evaluating Exclaimer Mail Utilities, then it may make sense for you to affect only messages from yourself to an external test account, e.g. a Hotmail account. You can change the scope later in the control panel." Below this text is a section titled "Scope" containing three radio button options: "All outgoing messages" (which is selected), "Only messages from" followed by a text input field and a browse button "...", and "to anyone" followed by a radio button and a text input field with a browse button "...". At the bottom of the window are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

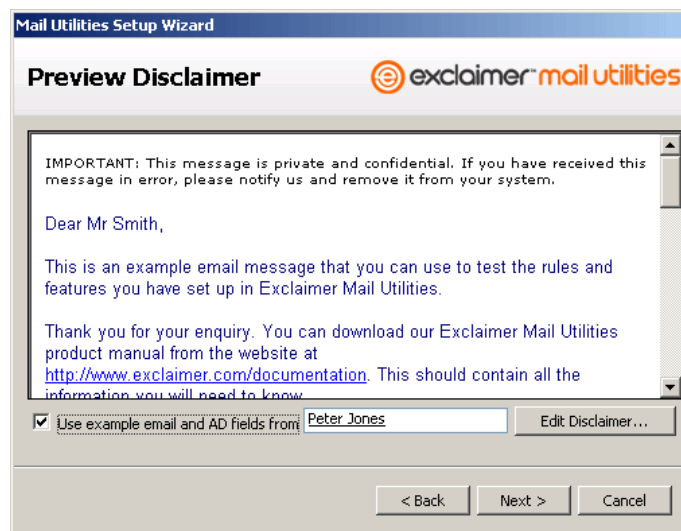
19. This step in the wizard only appears if you have enabled disclaimers.

This is where you can preview and edit your email disclaimer. You can preview your selected disclaimer with pre-populated information from your Active Directory. Enter the Active Directory user you want to use in the **Use example email and AD fields from** text box. Alternatively, you can view your disclaimer without pre-populated fields by un-checking the **Use example email and AD fields from** checkbox.

To edit your disclaimer click on the **Edit Disclaimer...** button. For more information on the **Disclaimer Editor** go to the **Disclaimer Editor** section.

You can also edit this disclaimer once Exclaimer Mail Utilities has completed its set up. You can also set up more advanced disclaimers that trigger on more specific criteria. For example, you could create a rule that adds a different disclaimer to email messages being sent to a specific domain.

Click on **Next >**.



**NOTE**

**Disclaimer Templates**

You can also select from a comprehensive list of disclaimer templates in the Exclaimer Mail Utilities Control Panel.

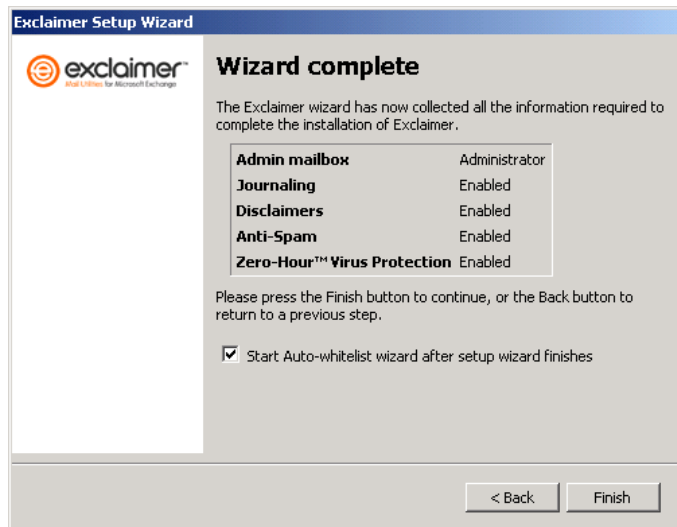
**Rules**

You can also set up more advanced rules for adding disclaimers once the product is fully installed and configured.

20. Enable the **Start Auto-Whitelist wizard after setup wizard finishes** checkbox if you want to start the Auto-Whitelist wizard. This checkbox only appears if you enabled Anti-Spam earlier in the wizard (it contains a tick by default). The Auto-Whitelist wizard is not available in Exclaimer Mail Utilities 2007.

To find out more about the Auto-Whitelist Wizard see *The Auto-Whitelist Wizard* section.

When you are happy with the settings you have chosen click on **Finish**.



Congratulations, you have now completed the Exclaimer Mail Utilities Setup Wizard.

## ▶ The Auto-Whitelist Wizard

This section describes how to navigate the Mail Utilities Auto-Whitelist Wizard.

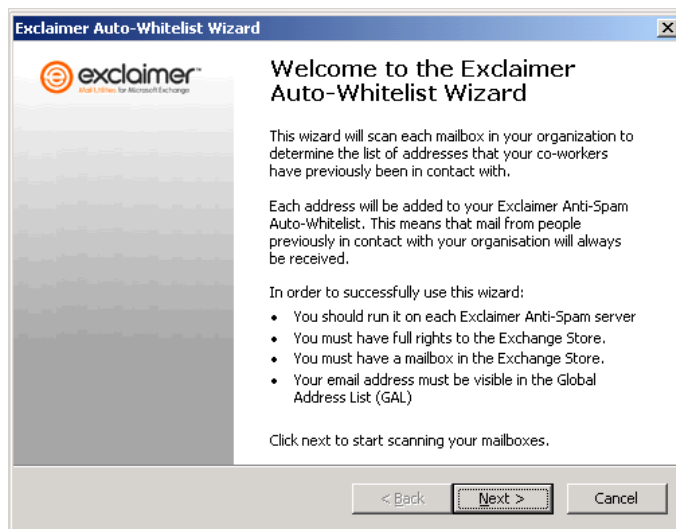
The Auto-Whitelist wizard identifies email addresses that your organization sends email to regularly and adds them to your Anti-Spam Auto-Whitelist. This guarantees that you will be able to receive email messages from clients that you are currently in email contact with.

**Note** – the Auto-Whitelist Wizard is not available in Exclaimer Mail Utilities 2007.

The Exclaimer Mail Utilities Auto-Whitelist Wizard should have started automatically after you clicked on **Finish** in the Setup Wizard. If the wizard didn't start you can start it manually. Click on the **Start** button, click on **Programs**, click on **Exclaimer** and click on **Auto-Whitelisting Wizard**.

### To configure the Auto-Whitelist using the Auto-Whitelisting Wizard

1. Click on **Next >**.



2. The Exclaimer Mail Utilities' Auto-Whitelist Wizard will scan your Exchange store finding all the email addresses that your organization has been in email contact with and adds them to the Auto-Whitelist.



3. Click on **View Contacts** to review the email addresses Exclaimer Mail Utilities has added to the Auto-Whitelist.

When you have finished, click on **Finish**. Mail Utilities will now incorporate this historic list of addresses into its database of automatically whitelisted senders.



Congratulations, you have now completed the Exclaimer Mail Utilities Auto-Whitelist Wizard. Once the Auto-Whitelist has been compiled by the wizard it cannot be amended. If you no longer want to receive email from a user or domain you can blacklist them.

Blacklist checks are performed before whitelist checks therefore ensuring that blacklisted senders will be blocked.

# Chapter 2

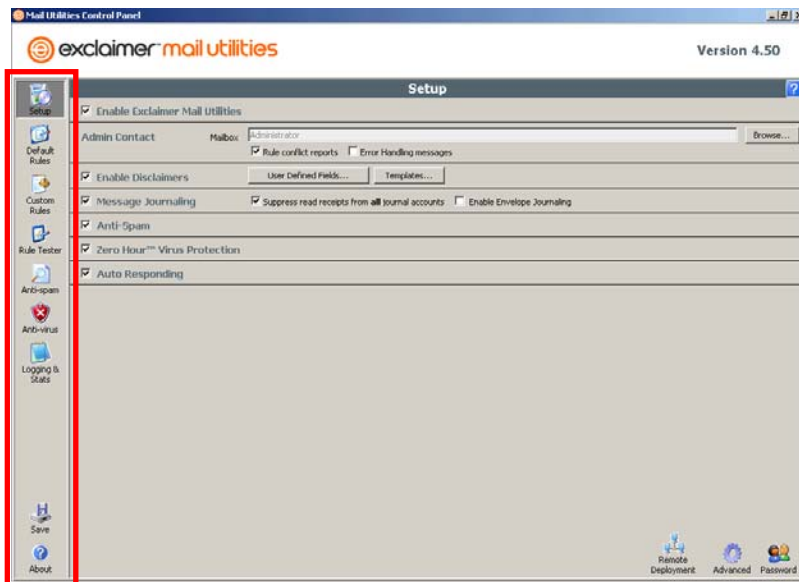
## Exclaimer Mail Utilities – The Control Panel

This chapter details the various menus and settings you can select and change in the Exclaimer Mail Utilities' control panel.

### ▶ Main menu

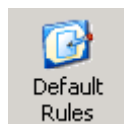
#### The Main menu

The main menu consists of a high level choice of options to control Exclaimer Mail Utilities' features.



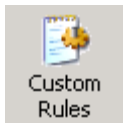
#### Setup

This menu allows you to control Exclaimer Mail Utilities' high level settings.



#### Default Rules

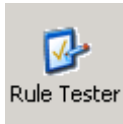
This menu allows you to modify and set up Exclaimer Mail Utilities' default disclaimers and message journaling rules.



Custom Rules

### **Custom Rules**

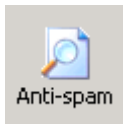
This menu allows you to add, amend or delete your own custom rules which can trigger features like disclaiming, auto-responding, delivery options or message journaling.



Rule Tester

### **Rule Tester**

This menu allows you to test the default rules and any custom rules you have set up before you actually deploy them.



Anti-spam

### **Anti-spam**

This menu allows you to set up and maintain Exclaimer Mail Utilities' anti-spam features.



Anti-virus

### **Anti-virus**

This menu allows you to set up and maintain Exclaimer Mail Utilities anti-virus features.



Logging & Stats

### **Logging & Stats**

This menu allows you to view all the data logging and statistics for Exclaimer Mail Utilities' systems.



Save

### **Save**

This button allows you to save any changes you have made to Exclaimer Mail Utilities' settings.



About

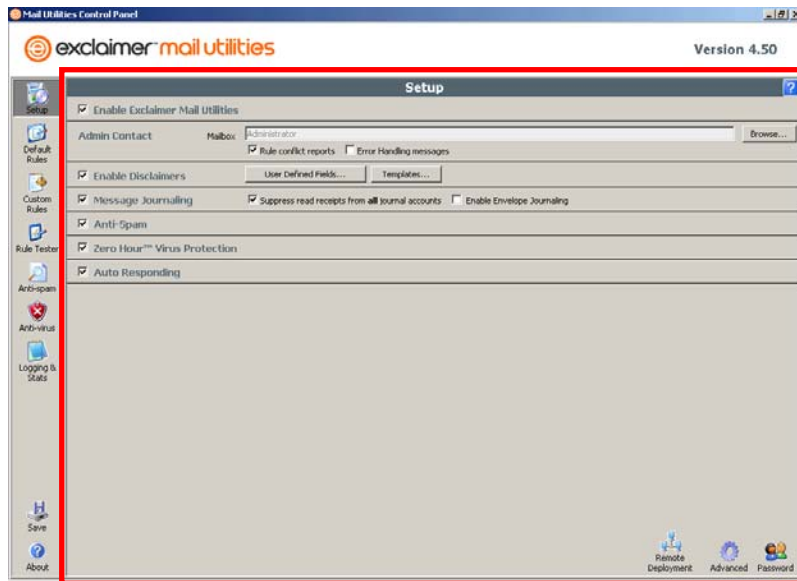
### **About**

This menu displays application information and is where you apply Exclaimer Mail Utilities' product license.

## ▶ Setup panel

### The Setup panel

The Setup panel is where you can control all the main features of Exclaimer Mail Utilities.



#### Enable Exclaimer Mail Utilities

You can use this option to quickly enable or to disable Exclaimer Mail Utilities' rules and features.

#### Admin Contact

This should specify an email account where all rule conflict reports, error handling messages and other admin messages Exclaimer Mail Utilities sends are received and monitored.

**Rule Conflict Reports** – Place a tick in this checkbox if you want rule conflict reports sent to your admin contact email account. These are sent when one of your custom rules is in conflict with another. For example, if you create a rule that adds a disclaimer when the sender is Anyone Internal and the recipient is Anyone, and another rule that states not to add a disclaimer when the sender is Anyone and the recipient is an Active Directory user. This will generate the following conflict report:

```
Exclaimer had a rule conflict between
```

```
Sender      : Anyone internal
Recipient   : Anyone
```

```
and
```

Sender : Anyone  
Recipient : Administrator  
(Administrator@exclaimer.local and aliases)

For the feature Disclaiming

The rule from Anyone internal to anyone won the contest as the feature was enabled for this rule.

To avoid rule conflicts for this sender and recipient pair, you should create an explicit rule for them.

**Error Handling Messages** – Place a tick in this checkbox if you want error handling messages sent to your admin contact email account. See the *Error Handling* tab in the *Advanced Settings* section for more information on the different types of error messages Exclaimer Mail Utilities can generate.

### **Enable Disclaimers**

You can use this feature to turn Exclaimer Mail Utilities' email disclaimers on or off. You can amend the default disclaimers in the Default Rules panel

### **User Defined Fields**

Clicking on this button opens the Edit User Defined Fields box. It allows you to edit existing User Defined Fields and create new or delete old User Defined Fields.

A User Defined Field is a field that you can insert your own text, images and formatting in, which can then be included in your organization's disclaimers, signatures and email templates. These fields can be updated from a single location and once changed will update in all the locations where they are used.

### **Templates**

This is where you can create your own customized templates based on existing Exclaimer Mail Utilities' templates. It is a much easier and quicker way of creating email templates without having to start from scratch.

Email templates lets you combine disclaimers, signatures, branding and layout providing you with reusable and professional looking email.

### **Message Journaling**

You can use this option to enable or disable message journaling. You can set up your message journaling options in the Default Rules panel.

Message journaling allows you to BCC all the emails your organization receives to a specified email account.

### **Suppress read receipts from all journal accounts**

Place a tick in this box to prevent read receipts being sent when a journaled email is read in the journal mailbox's inbox.

### **Enable Envelope Journaling**

Place a tick in this box to enable envelope journaling. This embeds the original message within a new message that simply contains a list of all the correspondents (sender and all individual recipients) in the embedded message. This option should be enabled when using Exclaimer Mail Utilities in tandem with the Exclaimer Mail Archiver package as it preserves all the sender and recipient data required for legal compliance purposes.

Enabling envelope journaling is essential if you want to capture BCC information in your journaled email messages.

### **Anti-Spam**

You can use this option to enable or disable Exclaimer Mail Utilities' anti-spam filter. You can set up and refine Exclaimer Mail Utilities' anti-spam settings using the Anti-spam panel.

### **Zero-Hour™ Virus Protection**

You can use this option to enable or disable Exclaimer Mail Utilities' Anti-Virus protection. You can modify Exclaimer Mail Utilities' anti-virus settings in the Anti-virus panel.

### **Auto Responding**

You can use this option to enable or disable all auto responders.

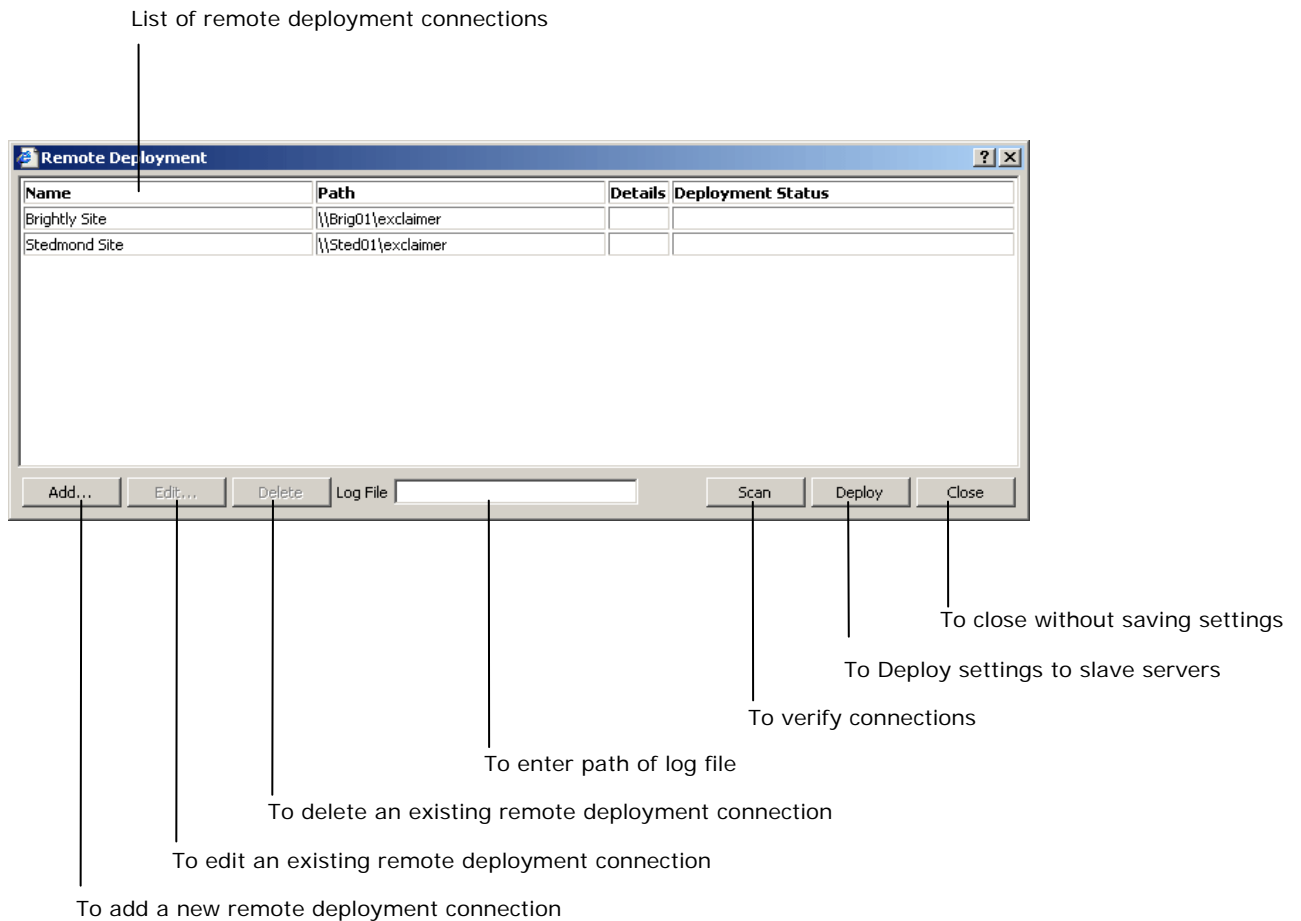
#### ***IMPORTANT!***

*To apply any changes you have made you must click on the **Save** icon in the left-hand menu.*

## ▶ Remote Deployment

### The Remote Deployment box

This dialog box contains the options that allow you to connect to other slave mail servers to upload settings from your main mail server.



The Remote Deployment table is divided up into four columns.

**Name** – Contains the names of the slave mail servers you have set up remote deployment for.

**Path** – Contains the path to the shared folder where the exclaimer.dll file can be found on each of your slave mail servers you have set up remote deployment for.

**Details** – Contains the version number of the **exclaimer.dll** file on your slave mail servers you have set up remote deployment for.

**Deployment Status** – Contains a report detailing the status of each slave mail server you have set up remote deployment for.

**Add...** - This button allows you to add a slave mail server to your remote deployment list.

**Edit...** This button allows you to edit the details of an existing slave mail server name and path.

**Delete** – This button allows you to delete an existing slave mail server entry.

**Log File** – This is where you enter the path detailing where you want the remote deployment log file stored. For example, 'c:\logging\RemoteDeploymentLog.txt'. Leave this field blank if you do not require a log to be stored.

**Scan** – This button allows you to validate the connections to your slave mail servers. It will also report the installation status on each of your configured servers.

**Deploy** – This button allows you to apply the settings from your master mail server to all your slave servers.

**Close** – This button closes the Remote Deployment dialog box.

## To set up Remote Deployment

1. Share the folder where the **exclaimer.dll** file is located on each of your slave mail servers that already have Exclaimer Mail Utilities installed.
2. Open the Exclaimer Mail Utilities Control panel.
3. Click on the **Setup** icon in the left-hand menu.
4. Click on the **Remote Deployment** icon in the bottom right of the **Setup** panel.
5. Click on the **Add...** button in the Remote Deployment dialog box.
6. Type the name of the server in the **Name** field and the UNC path where the **exclaimer.dll** file can be found. For example, '\\server2\Exclaimer'.

7. Click on **OK**.

## To set up a shared folder

1. On the remote server right click on the folder where the **eXclaimer.dll** is located.
2. Click on **Sharing and Security...**
3. Select the **Share this folder** radio button.
4. Click on **Permissions**.
5. Remove the **Everyone** group and add your Exchange administrator user or group, or the user who has access to the Exclaimer Mail Utilities Control panel.
6. Select the **Allow Full Control** checkbox.
7. Click on **Apply**, then click on **OK**.
8. Click on **Apply**, then click on **OK**.

## Deploy settings to slave mail servers

1. Open the Exclaimer Mail Utilities Control panel.
2. Click on the **Setup** icon in the left-hand menu.
3. Click on the **Remote Deployment** icon in the bottom right of the **Setup** panel.
4. Click on the **Deploy** button.
5. Click on **OK** in the Deployment complete dialog box.

**IMPORTANT!**

*We recommend that you use a UNC path rather than drive mappings for identifying the Path.*

*We recommend that you deploy in a multi-server environment from a single workstation to centralize the server management function.*

*If you wish to configure Exclaimer Mail Utilities from your workstation and then deploy the configuration to your servers, you will need a workstation license for the Control Panel. Contact [sales@exclaimer.com](mailto:sales@exclaimer.com) for more details.*

*Remote deployment between Exclaimer Mail Utilities 4.30 and Exclaimer Mail Utilities (2007) 4.50 is not possible. However, you can still remote deploy between Mail Utilities 4.30 and previous point releases. You can also remote deploy between Mail Utilities 4.50 and Mail Utilities 2007 systems.*

## ▶ Passwords

### The Set Password box

To set up or change the password to access Exclaimer Mail Utilities' Control Panel.

#### To add a password

1. Click on the **Password** icon in the bottom right-hand corner of the **Setup** panel.
2. Type in and confirm the password you want to use.
3. Click on **OK**.

#### To change your current password

1. Click on the **Password** icon in the bottom right-hand corner of the **Setup** panel.
2. Type in your current password and click on **OK**.
3. Type in and confirm the new password you want to use.
4. Click on **OK**.

#### To remove the password completely

1. Click on the **Password** icon in the bottom right-hand corner of the **Setup** panel.
2. Type in your current password and click on **OK**.
3. Leave the **Password:** and **Confirm:** fields blank.
4. Click on **OK**.

#### **IMPORTANT!**

*This password is purely to protect your Exclaimer Mail Utilities' configuration and is not used by any other product feature. It does not have to correspond to any other password on your computer and is not used by Exclaimer Mail Utilities to access other services.*

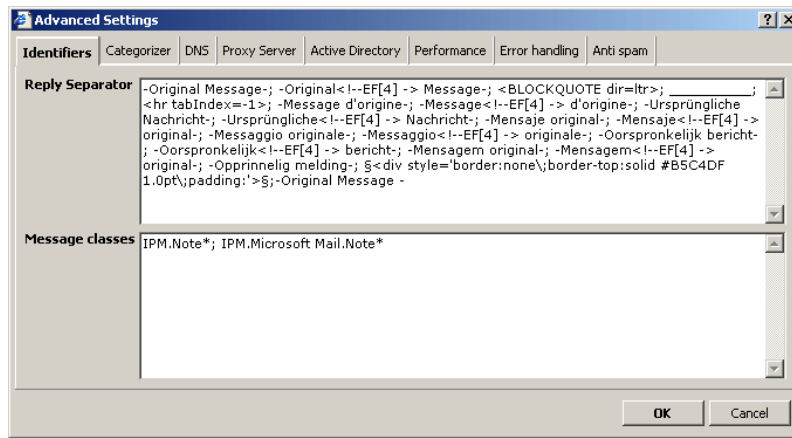
*We do not specifically recommend applying a password to your Exclaimer Mail Utilities' configuration. The configuration is already protected by the Windows security on the computer in question, which should suitably protect your Exclaimer Mail Utilities installation.*

## ▶ Advanced Settings

### The Advanced Settings box

Exclaimer Mail Utilities' advanced options panel allows you to configure a number of non-everyday Mail Utilities settings.

#### Identifiers tab



**Reply Separator** - contains the information that details how Exclaimer Mail Utilities identifies a reply or forwarded message in order to implement the reply above and reply below functionality used to insert disclaimers after a reply rather than at the end of the mail.

Should you need to change this you can do so by entering a semi-colon (;) separated list of text strings that are used to separate replies from the original messages by your mail client.

#### Reply Separator Key:

The following will explain how Exclaimer Mail Utilities interprets certain characters in the reply separators list.

#### Underscores

'\_' – will look for one or more consecutive underscores.

'\_\_' – will look for two underscores one after the other followed by more consecutive underscores.

'\_\_\_' – will look for three underscores one after the other followed by more consecutive underscores. etc.

## Hyphens

'-' – will look for one or more consecutive hyphens.

'--' – will look for two hyphens one after the other followed by more consecutive hyphens.

'---' – will look for three hyphens one after the other followed by more consecutive hyphens.

When searching for a specific string '-Original Message-' Exclaimer Mail Utilities will match one or more hyphens at the beginning and end of the text 'Original Message'. It will also accept a trailing line space at the end of the one or more hyphens before the text 'Original Message'. For example, Exclaimer Mail Utilities will match:

'-----Original Message-----'

'--- Original Message ---'

'- Original Message -'

## HTML tags

Exclaimer Mail Utilities can resolve HTML tags as reply separators. It matches first the element, then the attribute (if present in search string) and finally the attribute value (again, if present in search string).

Matches element then...

<hr tabIndex=-1>

matches attribute then...

<hr tabIndex=-1>

matches attribute value.

<hr tabIndex=-1>

Example:

<hr tabIndex=-1>

For this text string Exclaimer Mail Utilities will match any horizontal rule with a tabIndex that equals -1. However, the horizontal rule can include other attributes and values but it must have the attribute and value tabIndex=-1.

Match

<hr tabIndex=-1 color=#333333 size=1>

<hr color=#333333 tabIndex=-1>

Doesn't match

<hr tabIndex=-2>

## Style attribute

Style tags are resolved using a similar logic.

Example:

```
<div style='border:none\;border-top:solid #B5C4DF 1.0pt\;padding:'>
```

For this text string Exclaimer Mail Utilities will match any div tag that contains the style attribute with the following attributes and values 'border:none\;border-top:solid #B5C4DF 1.0pt\;padding:'.

The div tag can include other attributes but it must include the attribute and values style='border:none\;border-top:solid #B5C4DF 1.0pt\;padding:'. The style attribute can include other formatting attributes. For example, font-family:arial,tahoma or color:#FFFFFF.

Match

```
<div style='border:none;border-top:solid #B5C4DF 1.0pt;padding:10pt 0pt 0pt 10pt'>  
<div id=default style='border:none;border-top:solid #B5C4DF 1.0pt;padding:10pt 0pt 0pt 10pt'>
```

Doesn't match

```
<div style='border:solid #333333 1.0pt'>
```

**IMPORTANT!**

'\' – allows you to escape characters. For example, the semi-colon is used to separate the list of text strings that Exclaimer Mail Utilities uses to search for reply separators. However, it is also used as a separator within the style attribute of an HTML tag. To preserve these semi-colons without Exclaimer Mail Utilities seeing it as the next text string to search you must insert a backslash before the semi-colon '...border:none\;border-top:...'

**Spaces**

' ' - will look for one or more consecutive spaces.

When searching for a specific string '-Original\_Message-' Exclaimer Mail Utilities will match one or more spaces, if a tab appears within the space and if a space rolls over into a line break.

For example, Exclaimer Mail Utilities will match:

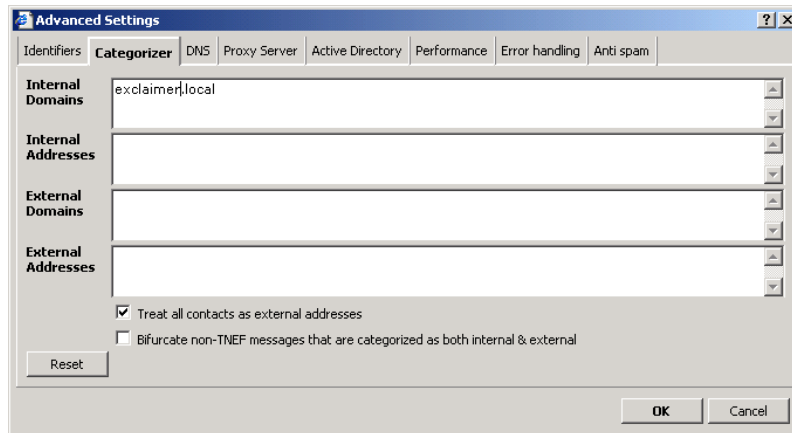
```
'-Original Message-'  
'-Original Message-'  
'-Original  
Message-'
```

**Message Classes** – This contains information that details what Exclaimer Mail Utilities will add disclaimers to. By

default, Exclaimer Mail Utilities will disclaim mail messages but not appointments, tasks etc. We recommend that you do not modify this list unless directed to by Exclaimer support.

Should you need to change this you can do so by entering an appropriate list of MAPI message classes separated by a semi-colon (;) that you want Exclaimer Mail Utilities to disclaim.

## Categorizer tab



This tab allows you to override how Exclaimer Mail Utilities categorizes emails as internal, outgoing or incoming. These settings are used by the Rules Processor to differentiate between internal, incoming and outgoing email messages.

**Internal Domains** – where you enter the SMTP domains that you are authoritative for. This will usually be your organization's primary domain (including the ubiquitous .local). It may also contain other domains that you have pre-filled in your Exchange Administration or IIS setup. Email addresses that end in these domains will be considered as internal addresses.

**Internal Addresses** – where you enter specific email addresses that you want categorized as internal, that would otherwise have been categorized as external. This is used to define the Anyone Internal option in the **Addressing** tab of the **Add Mail Rule** box, see *Add Mail Rule box* section.

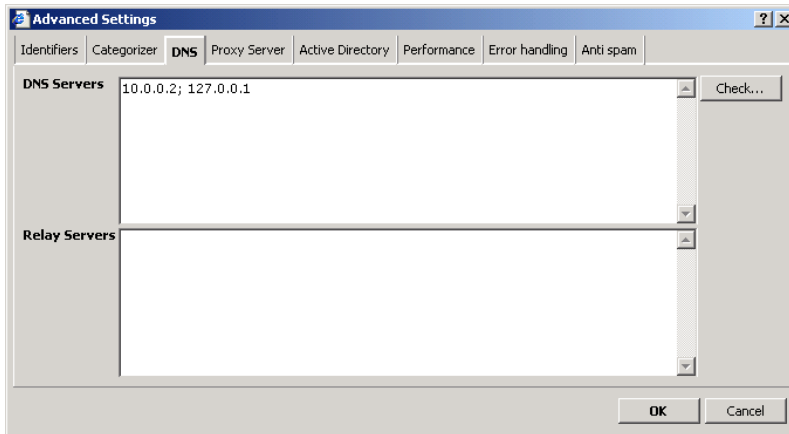
**External Domains** – where you enter a list of domains that you want categorized as external, that would otherwise have been categorized as internal.

**External Addresses** – where you enter a list of specific email addresses that you want categorized as external, that would otherwise have been categorized as internal.

**Treat all contacts as external addresses** – You use this checkbox to change the way your contacts are treated by Exclaimer Mail Utilities. Remove the tick from this checkbox to force Exclaimer Mail Utilities to treat all the contacts in your Active Directory as external when categorizing an email. Place a tick in this checkbox to make Exclaimer Mail Utilities treat your Active Directory contacts as internal.

**Bifurcate non-TNEF messages that are categorized as both internal and external** – Leave this option unchecked (without a tick) unless instructed to change it by Exclaimer Technical Support.

## DNS tab



These settings are only used by Exclaimer Mail Utilities' anti-spam and anti-virus modules to check and validate email messages from external domains.

**DNS Servers** – for specifying the DNS Servers you use to retrieve MX records for checking the authenticity of sending mail agents. Entering other servers can help to reduce loading on the default DNS servers.

You can add or change the DNS servers you use for checking MX records by entering their IP addresses in this field.

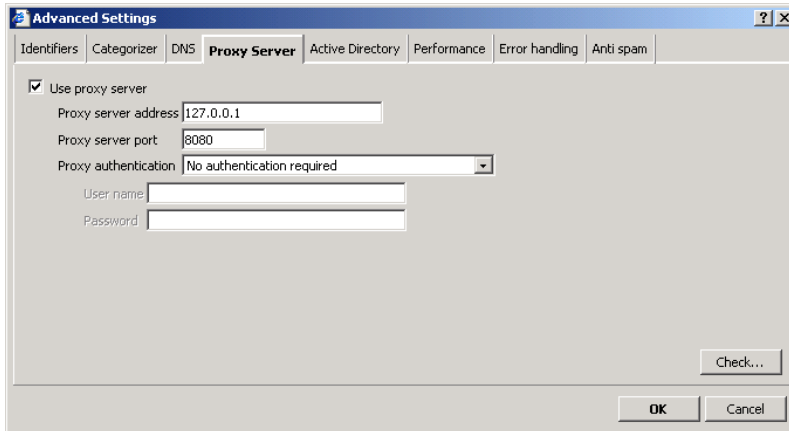
**Relay Servers** – a list of servers (IP Addresses) that you control which may relay mail into your domain.

Exclaimer Mail Utilities uses this list of servers to establish which agents in an SMTP conversation it should trust and which it should attempt to validate.

**Check...** - to verify the DNS servers you specified in the DNS Servers field.

You do not need to add any MX servers that you host for domains that you are authoritative for. Exclaimer Mail Utilities automatically gathers this data from the DNS and the internal domains field.

## Proxy Server tab



The screenshot shows the 'Advanced Settings' dialog box with the 'Proxy Server' tab selected. The 'Use proxy server' checkbox is checked. The 'Proxy server address' field contains '127.0.0.1', the 'Proxy server port' field contains '8080', and the 'Proxy authentication' dropdown menu is set to 'No authentication required'. There are empty text boxes for 'User name' and 'Password'. A 'Check...' button is located at the bottom right of the dialog, and 'OK' and 'Cancel' buttons are at the bottom center.

If you are using a Proxy server this is where you enter the details of the Proxy server you are using to access the Internet.

If you are using a proxy server, Exclaimer Mail Utilities will require this information to contact the Anti-Spam and Anti-Virus detection centers.

**Use Proxy Server** – Place a tick in this checkbox if you are using a Proxy server to access the Internet.

**Proxy Server Address** – This is where you enter the IP address, FQDN or NETBIOS name of your Proxy Server.

**Proxy Server Port** – This is where you enter the port number you use to communicate with your Proxy Server.

**Proxy Authentication** – This is where you select the type of authentication your Proxy Server requires (if any).

**User name/Password** – This is where you enter a user name and password for your proxy server should you select anything other than 'No authentication required' in the **Proxy Authentication** field.

**Check...** – You use this button to verify that Exclaimer Mail Utilities can reach the anti-spam and anti-virus detection center.

## Active Directory

The screenshot shows the 'Advanced Settings' dialog box with the 'Active Directory' tab selected. The 'Global Catalog' field is empty, with a note below it: 'Leave blank to use best global catalog server'. The 'Domain Controller' field is also empty, with a note: 'Leave blank to use best domain controller'. There is a checked checkbox for 'Cache the Active Directory search objects' and a 'TTL' field set to '5' minutes. Below these is a 'Credentials' section with fields for 'Login', 'Password', and 'Domain', and a note: 'Leave all fields blank to use LocalSystemAccount (or the account that the SMTP service is logged in as)'. 'OK' and 'Cancel' buttons are at the bottom right.

In normal operation we recommend you leave these fields blank. If you do this Exclaimer Mail Utilities will use appropriate defaults when querying your Active Directory. However, you can enter information to manually override Exclaimer's defaults.

### **IMPORTANT!**

*If you change any of the default settings here you run the risk of Exclaimer Mail Utilities failing to work properly. You must be confident that any changes you make will not affect the normal operation of Exclaimer Mail Utilities. For example, if the Global Catalog you have set manually goes offline Exclaimer Mail Utilities may fail to process email. If you leave the Global Catalog field blank it will automatically find another GC should the one it is currently using go offline.*

**Global Catalog** – This is where you can enter the FQDN of the Global Catalog Server that Exclaimer Mail Utilities will use in Active Directory queries. For example,  
**GC:\\gcservername.domain.local**

**Domain Controller** – This is where you enter the FQDN of The Domain Controller that Exclaimer Mail Utilities will use to contact the Domain Controller. This can be a server name or a domain name. For example,  
**DC:\\dcservername\domain.local**

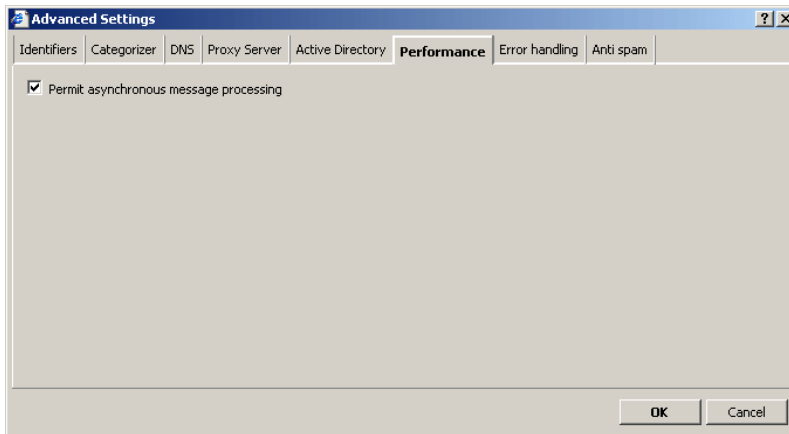
**Cache the Active Directory search objects** – Place a tick in this checkbox to cache the Active Directory search objects.

**TTL:** - This is where you enter the amount of time between caches. Exclaimer Mail Utilities will normally cache the information used to find the best catalog server for 5 minutes for performance reasons. After this time it will refresh the information and may choose a different catalog server.

**Credentials** – This is where you enter the information required to log into a specific domain controller. It is important to ensure that the credentials supplied have adequate read access to the Active Directory.

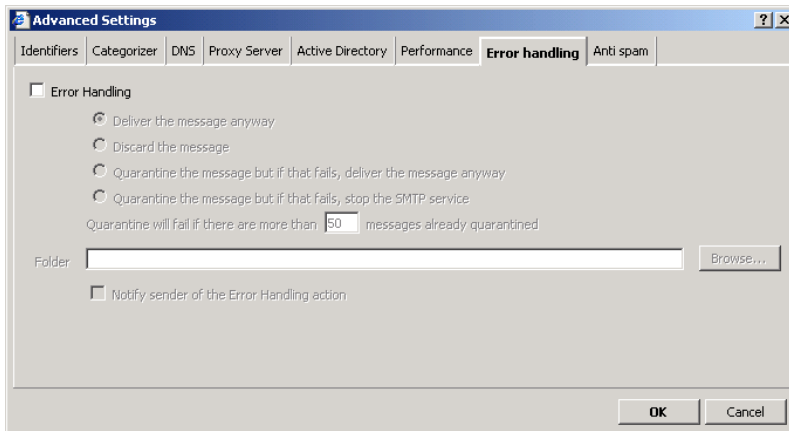
You should only use this option when instructed to by Exclaimer Technical Support.

## Performance tab



This tab displays the processing settings for Exclaimer Mail Utilities. DO NOT modify this setting unless instructed to by Exclaimer Technical Support.

## Error Handling tab



This is where you configure how Exclaimer Mail Utilities behaves when an error is encountered.

**Error Handling** – Place a tick in this checkbox to enable error handling.

**Deliver message anyway** – Select this option if you want Exclaimer Mail Utilities to deliver email messages that it has not been able to process.

**Discard the message** – Select this option if you want Exclaimer Mail Utilities to discard messages that it has not been able to process.

**Quarantine the message but if that fails, deliver the message anyway** – Select this option if you want Exclaimer Mail Utilities to deliver email messages that it has not been able to process and has failed to write to the quarantine folder.

**Quarantine the message but if that fails, stop the SMTP service** – Select this option if you want Exclaimer Mail Utilities to stop the SMTP service if it has not been able to process an email message and has failed to write to the quarantine folder. By stopping the SMTP service Exclaimer Mail Utilities will not allow the email message to be delivered.

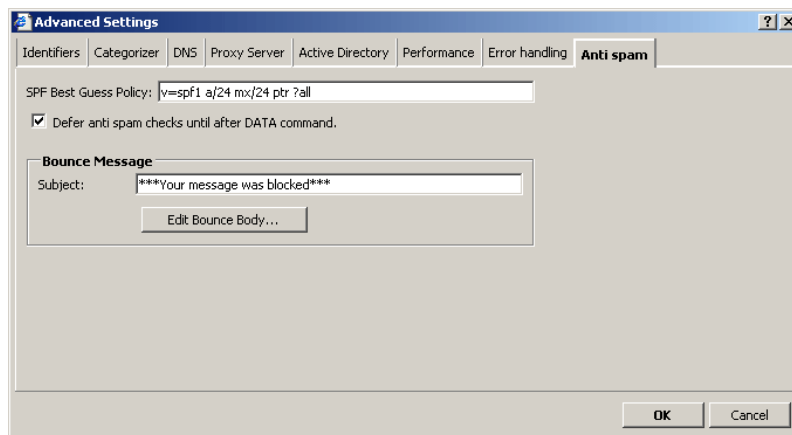
**Quarantine will fail if there are more than # messages already quarantined** – This is where you set the number of email messages that your quarantine folder will accept before it fails. By default this is set at 50.

**Folder** – This is where you select the folder you want Exclaimer Mail Utilities to store quarantined (unprocessed) email messages.

**Notify Sender of the Error Handling Action** – Place a tick in this checkbox to send an email to the original sender telling them that their email message has failed.

If you have configured Error Notifications to be sent to the admin contact, the admin contact will receive a similar message.

## Anti-Spam



This is where you configure Exclaimer Mail Utilities' SPF Best Guess Policy and when it performs its Anti-Spam checks. You can also edit the contents of Exclaimer Mail Utilities' bounce email.

**SPF Best Guess Policy:** - This is where you will find the default SPF which states that if the message is received

from an IP address in the /24 net block of your MX server or an A record in DNS or a PTR in their domain, then this will presume the sender to be an SPF pass.

SPF is a special format of DNS text record which details the email servers authorized to send email and helps to identify faked or spoofed email messages. By referring to the SPF policy that the domain owner has published Exclaimer Mail Utilities can identify whether an email message has been sent from an authorized email server.

**Defer anti-spam checks until after DATA command –**  
Place a tick in this option if you want Exclaimer Mail Utilities to defer its spam checks until after it has received the DATA command.

Exclaimer Mail Utilities will classify a message as spam as soon as it has all the data it needs to do so. Exclaimer Mail Utilities usually defers processing of this classification until the entire message has been received (which in SMTP protocol terms, is after the DATA command has been completed). In some cases Exclaimer Mail Utilities will block a sender before it reaches the DATA command. You can force Exclaimer Mail Utilities to wait until after the DATA command using this option.

Using this option can make the whitelist and backdoor more effective as Exclaimer Mail Utilities waits until it has received the whole message before it performs any spam checks.

This option also allows you to treat both email messages sent directly to you or those relayed via a secondary MX server equally, helping to minimize false positives.

Choosing to defer spam checks until after the DATA command does not affect Exclaimer Mail Utilities' spam blocking rate.

If you are worried about the bandwidth remove the tick from this option. When this option is unchecked Exclaimer Mail Utilities will perform some of its spam checks before DATA command therefore reducing the number of email messages you actually download.

**Bounce Message** - You use this area to edit the subject and contents of the bounce message, should an incoming email be rejected after the protocol has finished.

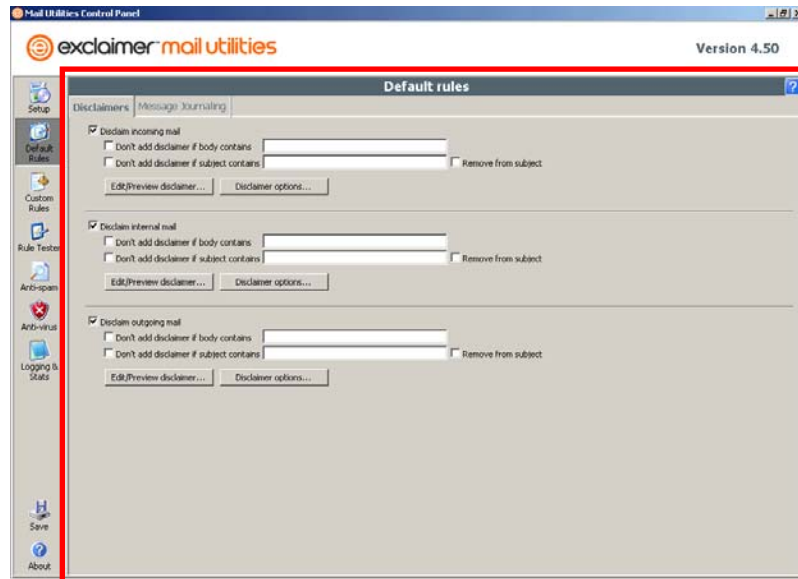
A bounce message is an email that is sent back to the original sender when their email message has been rejected by the Anti-Spam Engine and you have enabled the Bounced email message feature.

## ► Default Rules panel

### The Default Rules panel

#### Disclaimer tab

This tab is broken down into three sections:



**Incoming** – You can add a disclaimer to all incoming email messages. For example, you could use it to warn your employees that the email was received from outside the organization and may contain information that they find offensive. Alternatively, it can be used for regulation compliance.

**Internal** – You can add a disclaimer or signature to all email messages sent internally. For example, you can use this to set up a standard signature for messages sent to users on your domain.

**Outgoing** – You can add a disclaimer to all email messages sent to external domains. For example, you can add legal disclaimers for regulation compliance purposes.

Each section contains options for specifying when the disclaimer should appear and for selecting or modifying the disclaimer that appears.

There is a main checkbox where you can select whether you want to apply the associated type of disclaimer.

**Don't add disclaimer if body contains** – you use this to identify if a disclaimer has already been added. For example, if you have a long email conversation and are sending email back and forth, using this option can stop multiple disclaimers being added to the email.

It is best to keep the phrase that Exclaimer Mail Utilities looks for short. Emails are reformatted by email software every time a reply is created or a mail is forwarded so a short distinctive phrase has more chance of surviving reformatting than a long one. The phrase must appear in the disclaimer. If it appears elsewhere this feature may not work. For example, it could be your organization's telephone number or perhaps your company registration number.

It is important to remember that this phrase is also case sensitive.

**Don't add disclaimer if subject contains** – you use this to send email messages without adding a disclaimer. You can configure Exclaimer mail Utilities to not add a disclaimer if the subject of an outgoing or internal email message contains a specific piece of text in the Subject field. For example, '[remove disclaimer]'. This will be identified by Exclaimer Mail Utilities and a disclaimer will not be added.

**Remove from subject** – you use this to remove the piece of text you used to prevent the disclaimer using the **Don't add disclaimer if subject contains** option. This ensures that the recipient will not see the '[remove disclaimer]' text in the message subject field.

**Edit/Preview disclaimer...** - you use this button to change the text in the disclaimer you have applied. It opens an Disclaimer Editor window that as well as allowing you to edit your disclaimer's format also allows you to preview your changes in HTML, RTF and Plain Text.

For more information on the Disclaimer Editor see the *Disclaimer Editor* section in *Appendix A*.

**Disclaimer options...** - this is where you set up the Encoding method and Character set used for both HTML and Text email disclaimers. You can also specify exactly how to attach disclaimers to normal, encrypted and digitally signed email.

For more information on the Disclaimer Options box see the *Disclaimer Options box* section in *Appendix A*.

**IMPORTANT!**

*If an email has multiple recipients some of which are internal and some of which are external, Exchange will bifurcate the email such that external recipients receive a mail with the external disclaimer and internal recipients receive the internal disclaimer.*

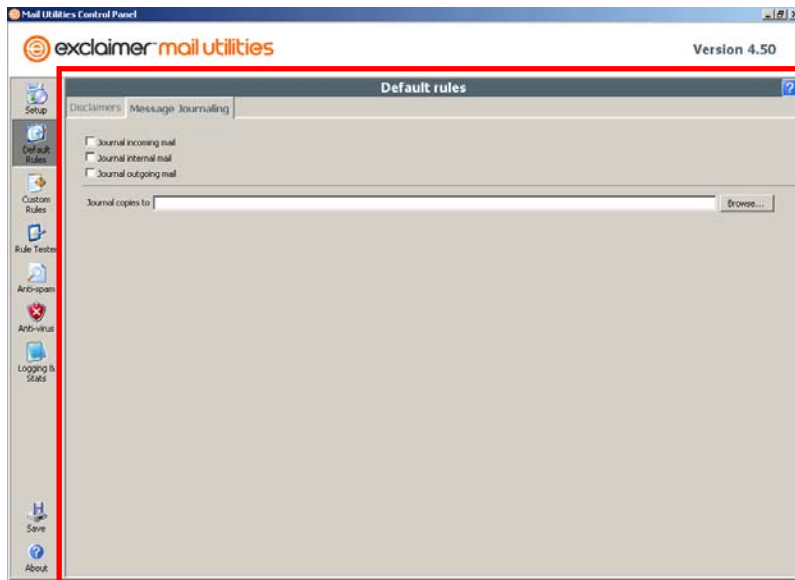
*If neither the sender nor the recipient of an email are in your Active Directory, and your server is relaying, then the email will be treated as incoming and outgoing and will trigger disclaiming options accordingly.*

*You can turn off disclaiming completely by opening the Exclaimer Mail Utilities' Control Panel, clicking the **Setup** icon and removing the tick from the **Enable Disclaimers** checkbox.*

*To apply any changes you have made you must click on the **Save** icon in the left-hand menu.*

## Message Journaling tab

This is where you set the types of email you want to journal.



**Journal incoming mail** – check this option to journal incoming mail to your specified mailbox.

**Journal internal mail** – check this option to journal internal mail to your specified mailbox.

**Journal outgoing mail** – check this option to journal outgoing mail to your specified mailbox.

**Journal copies to** – you use this to specify the email account you want the journaled email sent to.

### **IMPORTANT!**

*You can turn off message journaling completely by opening the Exclaimer Mail Utilities' Control Panel, clicking the **Setup** icon and removing the tick from the **Message Journaling** checkbox.*

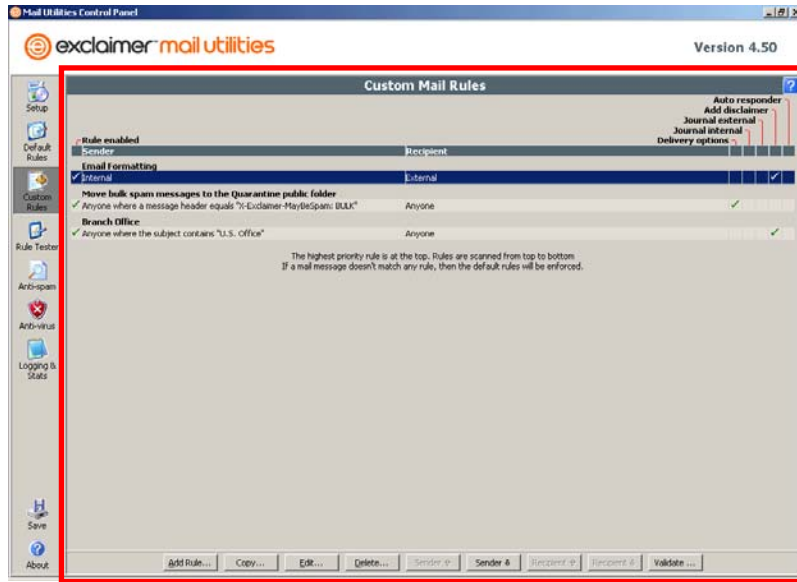
*We recommend that email is journaled to a dedicated account that is not in regular use. This avoids inadvertent responses from a journaling account.*

*To apply any changes you have made you must click on the **Save** icon in the left-hand menu.*

## ► Custom Rules panel

### The Custom Rules panel

This is where you can create your own custom rules.



**Add rule...** - You use this button to create a custom rule.

**Copy...** - You use this button to copy an existing custom rule. Select the rule you want to copy before clicking on this button.

**Edit...** - You use this button to modify an existing custom rule. Select the rule you want to edit before clicking on this button. The changing of a custom rule cannot be undone. Exit the control panel without clicking on the **Save** icon to cancel your changes.

**Delete** – You use this button to delete a custom rule. Select the rule you want to delete before clicking on this button. The deletion of a custom rule cannot be undone. Exit the control panel without clicking on the **Save** icon to cancel your changes.

**Sender ↑** - You use this button to increase the priority of the selected custom rule.

**Sender ↓** - You use this button to decrease the priority of the selected custom rule.

**Recipient ↑** - You use this button to increase the priority of the selected custom rule within a sender block. Rules are grouped first by sender, then by recipient. This option is

only available if there is more than one rule in a sender block.

**Recipient ↓** - You use this button to decrease the priority of the selected custom rule within a sender block. Rules are grouped first by sender, then by recipient. This option is only available if there is more than one rule in a sender block.

**Validate...** - You use this button to check whether the selected rule is valid. Some existing rules may be invalidated by changes in your Active Directory. All rules are validated when the Control Panel first starts.

**Key:**

✓ This indicates that the feature is triggered by the rule. It also indicates that a rule is enabled.

✗ This indicates that the feature will be blocked by the rule. It also indicates that a rule is disabled.

• This indicates that, although a rule has a custom feature set up it will not be triggered by the rule.

↓ This indicates that once the rule has finished processing the email message it will pass it on to the next applicable rule for that feature.

**IMPORTANT!**

*Custom rules are invoked before default rules. If a particular email does not match any custom rule, the default rules will be used.*

*Custom rules are checked in the order they appear from top to bottom.*

*Custom rules that specify 'anyone' as the sender or recipient will be processed last regardless of where they appear in the list.*

*If an email contains multiple recipients, the first custom rule that matches at least one recipient will be used.*

*You can use the Rule Tester to validate the custom rules that you create.*

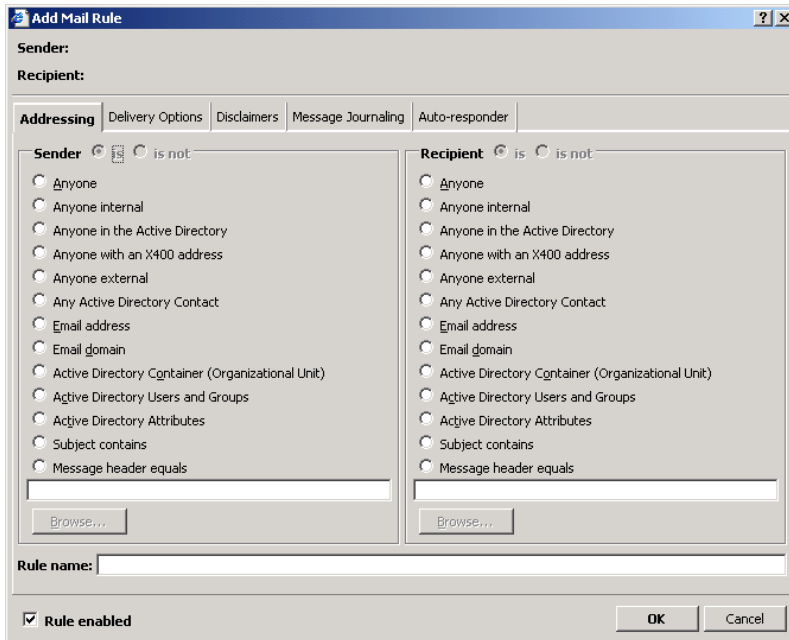
*To apply any changes you have made you must click on the **Save** icon in the left-hand menu.*

## ▶ Add Mail Rule box

### The Add Mail Rule box

This box is broken down into five tabs.

#### Addressing tab



The screenshot shows the 'Add Mail Rule' dialog box with the 'Addressing' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar, there are labels for 'Sender:' and 'Recipient:'. The main area is divided into two columns: 'Sender' and 'Recipient'. Each column has a radio button for 'is' and 'is not'. Below these are lists of options: 'Anyone', 'Anyone internal', 'Anyone in the Active Directory', 'Anyone with an X400 address', 'Anyone external', 'Any Active Directory Contact', 'Email address', 'Email domain', 'Active Directory Container (Organizational Unit)', 'Active Directory Users and Groups', 'Active Directory Attributes', 'Subject contains', and 'Message header equals'. Each list has a 'Browse...' button below it. At the bottom, there is a 'Rule name:' text box, a checked 'Rule enabled' checkbox, and 'OK' and 'Cancel' buttons.

This tab allows you to select the sender or recipient that you want Exclaimer Mail Utilities to check for when processing email messages.

#### Sender/Recipient

Both the Sender and Recipient sections have **is** and **is not** radio buttons. These allow you to specify whether the rule is looking to match or to not match the option you have chosen.

The Sender and Recipient sections present a selection of options that you can choose from:

**Anyone** – This is a wildcard and will match any sender or recipient.

**Anyone Internal** – This is a wildcard that will match any internal sender or recipient. This can be anyone who has an email address or domain that is included in the internal domain list.

**Anyone in the Active Directory** – This is a wildcard that will match any users in your Active Directory, including contacts. This can include both internal and external senders and recipients that exist in the Active Directory.

**Anyone with an X400 address** – This will match any user with an X400 address.

**Anyone External** – This is a wildcard that will match any external sender or recipient.

**Any Active Directory Contact** – This is a wildcard that will match any of your Active Directory Contacts.

**Email Address** – This is a specific email address. You type the email address you want to match in the text box above the **Browse...** button. For example, 'john.smith@exclaimer.com'. This selection also supports wildcards '\*.smith\*' or 'john.smith@exclaimer.\*'

**Email Domain** – This is a specific domain address. You type the domain address you want to match in the text box above the **Browse...** button. For example, 'exclaimer.com'. This selection also supports wildcards '\*.net' or 'exclaimer.\*'

**Active Directory Container (Organizational Unit)** – This will match a specific Active Directory Organizational Unit.

The **Browse...** button becomes active when this option is selected. You can use it to identify the Organizational Unit you want to match. You can add more than one organizational unit by repeating this process and clicking on the **No** button in the Exclaimer Mail Utilities' Control Panel warning dialog box to add a new container.

**Active Directory Users and Groups** – This will match any user or group from your active directory. For example, 'John Smith' or 'Accounts'. This automatically updates so if a new user is added to the Accounts group the rules that specify the Accounts group will also apply to the new user.

The **Browse...** button becomes active when this option is selected. You can use it to identify the user or group you want to match.

The **Get list of group members from a GC** checkbox will appear when this option is selected. If you place a tick in this checkbox Exclaimer Mail Utilities will resolve Group membership data from a Global Catalog rather than a Domain Controller.

**Active Directory Attributes** – This allows you to match specific Active Directory attributes and values.

The **Browse...** button changes into the **Settings...** button when this option is selected. You can use it to create the rule/query you want to resolve. See the *Active Directory Attribute Query Editor* section in *Appendix A*.

**Subject contains** – This will match text in the Subject field. This selection also supports wildcards *'\*enquiry\*'* or *'\*quote\*'*

The **Remove from Subject** checkbox will appear when this option is selected. If you place a tick in this checkbox, Exclaimer Mail Utilities will remove the text that it matches in the Subject field.

**Message header equals** – This will match text in the message header field. The general form of a message header is Field: Value. Exclaimer Mail Utilities allows you to specify either the Field or the Value and use an asterisk (\*) to perform wildcard matching.

For example, *\*chris\** would match emails received from anyone with the text *chris* contained anywhere in their email address or display name.

**The free text box at the bottom of the list** – This is where you enter the text, username, domain, etc. that you want to match. The text you type in this box is not case sensitive.

**Examples of text:**

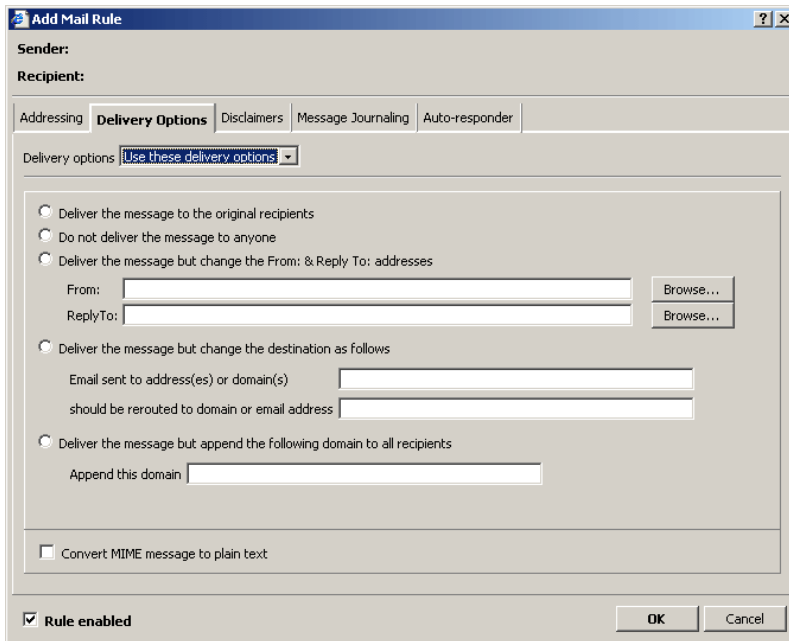
|   |  |
|---|--|
| <b>Email address</b>                                    | user.*@exclaimer.com<br><br>*@exclaimer.com  |
| <b>Email Domain</b>                                     | exclaimer.*<br><br>*.co.uk   |
| <b>Active Directory Container (Organizational Unit)</b> | Container Exclaimer.local/Users  |
| <b>Active Directory Users and Groups</b>                | Administrator<br>(Administrator@exclaimer.com and aliases)<br><br>Accounts (Exclaimer.local) |

**Rule name:**

This is where you enter the name of your custom rule. It is best to name the rule with a description that helps to identify what the rule does. You may also find it useful to enter when changes were made to a rule, if you have many people administering your server.

**Rule enabled** – This checkbox appears on all tabs and allows you to deactivate the rule without having to remove or delete it.

## Delivery Options tab



The screenshot shows the 'Add Mail Rule' dialog box with the 'Delivery Options' tab selected. The dialog has a title bar with a question mark and close button. Below the title bar are fields for 'Sender:' and 'Recipient:'. The 'Delivery Options' tab is active, showing a dropdown menu for 'Delivery options' set to 'Use these delivery options'. There are four radio button options: 'Deliver the message to the original recipients', 'Do not deliver the message to anyone', 'Deliver the message but change the From: & Reply To: addresses' (with 'From:' and 'ReplyTo:' text boxes and 'Browse...' buttons), and 'Deliver the message but change the destination as follows' (with 'Email sent to address(es) or domain(s)' and 'should be rerouted to domain or email address' text boxes). A fifth radio button option is 'Deliver the message but append the following domain to all recipients' (with 'Append this domain' text box). At the bottom, there is a checkbox for 'Convert MIME message to plain text' and a checked checkbox for 'Rule enabled'. 'OK' and 'Cancel' buttons are at the bottom right.

**Delivery Options** – This allows you to select between **Ignore this rule**, **Use these delivery options** and **Don't use delivery options**.

**Deliver the message to the original recipients** – This delivers the email message to its original recipients.

**Do not deliver the message to anyone** – This stops the message being delivered to anyone. The message is destroyed so no copy is stored.

**Deliver the message but change the From: and Reply To: addresses** – This allows you to change the email message's **From:** and **Reply To:** fields so that you can specify a different sender and/or email address the recipient replies to.

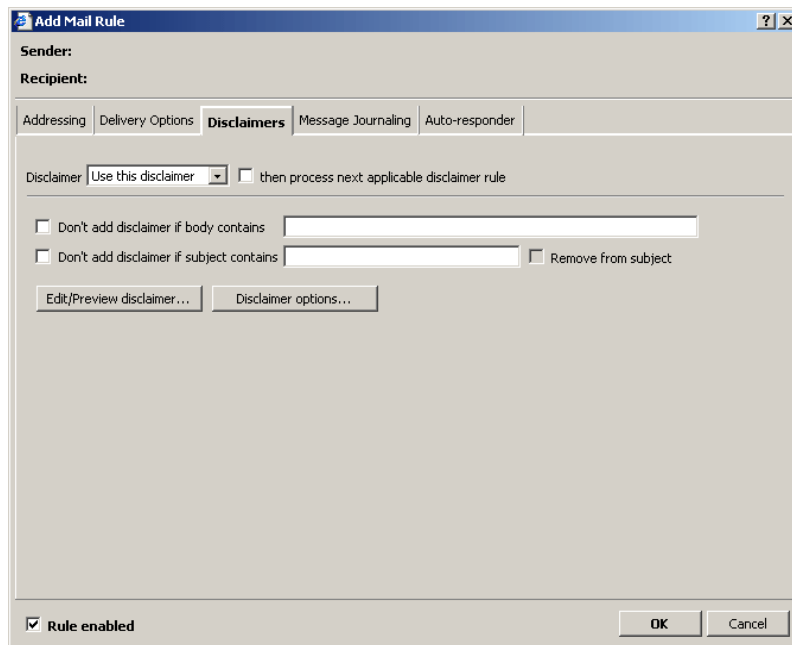
**Deliver the message but change the destination as follows** – This allows you to change where email messages

are being sent. Email sent to a specific email address or domain can be rerouted to an alternative email address or domain. You can use wildcards to specify all email addresses or all domains.

**Deliver the message but append the following domain to all recipients** – This will append another domain on to the recipient's email addresses. For example, peterj@exclaimer.com.anotherdomain.com.

**Convert MIME message to plain text** – This checkbox allows you to convert HTML or RTF MIME messages you send or receive into plain text email messages.

### Disclaimers tab



**Disclaimer** – This allows you to select between **Ignore this rule**, **Use this disclaimer** and **Don't add disclaimer**.

**then process the next applicable disclaimer rule** – Placing a tick in this checkbox ensures that Exclaimer Mail Utilities will process the next disclaimer rule in the list, adding further disclaimers where applicable.

**Don't add disclaimer if body contains** – You can use this to ensure that you don't add more than one disclaimer to an email that includes multiple replies.

It is best to keep the phrase that Exclaimer Mail Utilities looks for short. Emails are reformatted by email software every time a reply is created or an email is forwarded. A

short distinctive phrase has more chance of surviving reformatting than a long one. The phrase must appear in the disclaimer. If it appears elsewhere this feature may not work. It is important to remember that this phrase is also case sensitive.

**Don't add disclaimer if subject contains** – This doesn't add a disclaimer to email messages that contain a specific piece of text in the **Subject** field.

The **Remove from Subject** checkbox will become active when this option is selected. If you place a tick in this checkbox, Exclaimer Mail Utilities will remove the text that it matches in the Subject field.

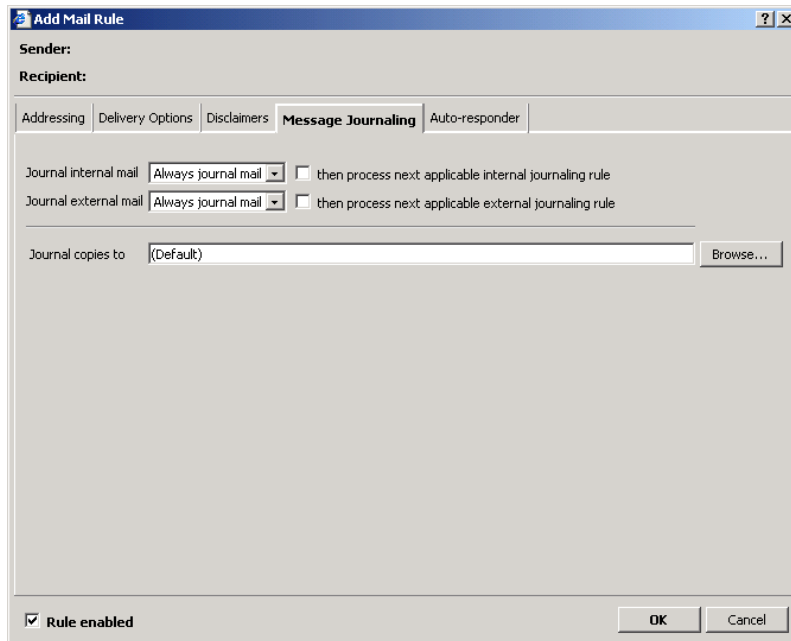
**Edit/Preview disclaimer...** - You use this button to change the text in the disclaimer you have applied. It opens the Disclaimer Editor window that as well as allowing you to edit your email's format, also allows you to preview your changes in HTML, RTF and Plain Text.

For more information on the Disclaimer Editor see the *Exclaimer's Disclaimer Editor* section in *Appendix A*.

**Disclaimer options...** - This is where you set up the Encoding method and Character set used for both HTML and Text email. You can also specify exactly how to attach disclaimers to normal, encrypted and digitally signed email.

For more information on the Disclaimer Options box see the *Disclaimer Options box* section in *Appendix A*.

## **Message Journaling**



**Journal internal mail** – This allows you to select between **Ignore this rule**, **Always journal mail** and **Never journal mail**.

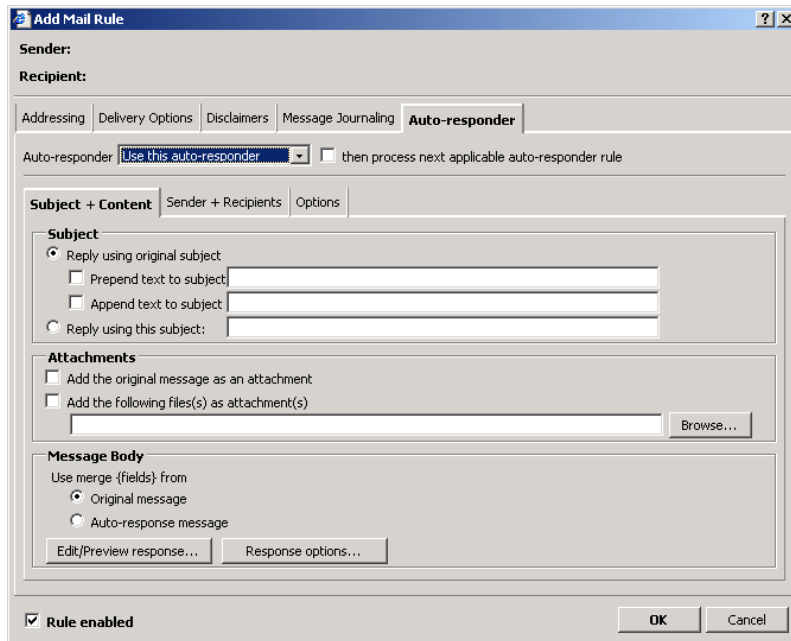
**then process next applicable internal journaling rule** – Placing a tick in this checkbox ensures that Exclaimer Mail Utilities will process all the remaining internal mail journaling rules, journaling to further mailboxes where applicable.

**Journal external mail** – This allows you to select between **Ignore this rule**, **Always journal mail** and **Never journal mail**.

**then process next applicable external journaling rule** – Placing a tick in this checkbox ensures that Exclaimer Mail Utilities will process the next external mail journaling rule, journaling to further mailboxes where applicable.

**Journal copies to** – This allows you to select the mailbox you want to journal your mail to. For example, you can create two custom rules to specify that emails between certain departments are journaled to one mailbox, whilst external emails from another department are journaled to a different mailbox.

#### **Auto-responder tab**



**Auto-responder** – This allows you to select between **Ignore this rule**, **Use this auto-responder** and **Don't use an auto-responder**.

**then process next applicable auto-responder rule** – Placing a tick in this checkbox ensures that Exclaimer Mail Utilities will process all the remaining auto-responder rules, ensuring that all the remaining auto-responders are processed.

The Auto-responder tab is broken down into three sub-tabs. These are divided as follows:

#### **Subject + Content sub-tab**

**Subject** – This allows you to select exactly what you want to appear in the Subject field of the auto-response.

**Reply using original subject** – This replies to the sender with the subject of their original email in the subject of the auto-response.

**Prepend text to subject** – With this option you can add text before the subject in the auto-response. For example, 'RE: ...'.

**Append text to subject** – With this option you can add text after the subject in the auto-response.

**Reply using this subject** – This allows you to specify your own reply subject.

**Attachments** – This allows you to insert attachments into the auto-response message.

**Add the original message as an attachment** – Place a tick in this checkbox to add the original message as an attachment.

**Add the following file(s) as attachment(s)** – Place a tick in this checkbox to specify the location of the file(s) you want to attach to the auto-response message. You can add multiple attachments by separating each full path with a semi-colon (;). For example, 'c:\email\file1.pdf;c:\email\file2.pdf'.

**Message Body** – This allows you to edit the auto-response message and specify whether you want to use the {fields} from the original message or from the auto-response message.

**Use merge {fields} from...**

{fields} take data from the sender's email message and allow you to use it in the auto-responder. For example, you could use the sender's Display Name to personalize the auto-responder's content.

**Original message** – This means that you can utilize the {fields} from the message of the original sender. For example, you can include their SMTP address.

**Auto-response message** – This can use fields from your Active Directory or the fields contained within the sender's original email message. These can then be used to personalize the auto-response.

**Edit/Preview response...** - This button allows you to create/edit the content of the auto-responder.

**Response options...** - This is where you set up the Encoding method and Character set used for both HTML and Text email.

**Sender + Recipients sub-tab**

This is where you can specify the sender and who receives the auto-response.

**Send auto-response to original sender** – This sends the auto-response to the original sender.

**Send auto-response to:** - This sends the auto-response to a specific email address of your own choosing.

**Auto-response should appear to be from:** - This is where you can enter the email address that you want the auto-response to appear from.

**Auto-response reply-to address:** - This is where you can specify the email address that you want the recipients to reply to.

**CC Auto-response to:** - This is where you can specify the email address you want to send a carbon copy of the auto-response to.

**BCC Auto-response to:** - This is where you can specify the email address you want to send a blind carbon copy of the auto-response to.

## Options sub-tab

**Message format - Provide auto-response message body as... Plain text, HTML or Both** – This is where you can specify the format of your auto-response email message.

**Loop detection** – This is where you can specify the number of auto-responses sent to a sender within a certain period of time. For example, by default Exclaimer Mail Utilities will only send 10 auto-responses in a 60 minute period to the same sender. You can increase or decrease both the number of auto-responses sent and the time period.

### **IMPORTANT!**

*Auto-responders can be applied to outgoing, internal and incoming emails*

*Use the Rule Tester to check how your auto-responses will look.*

*You can disable the Auto-responders feature by opening the **Exclaimer Mail Utilities' Control Panel**, clicking the **Setup** icon and removing the tick from the **Auto Responding** checkbox.*

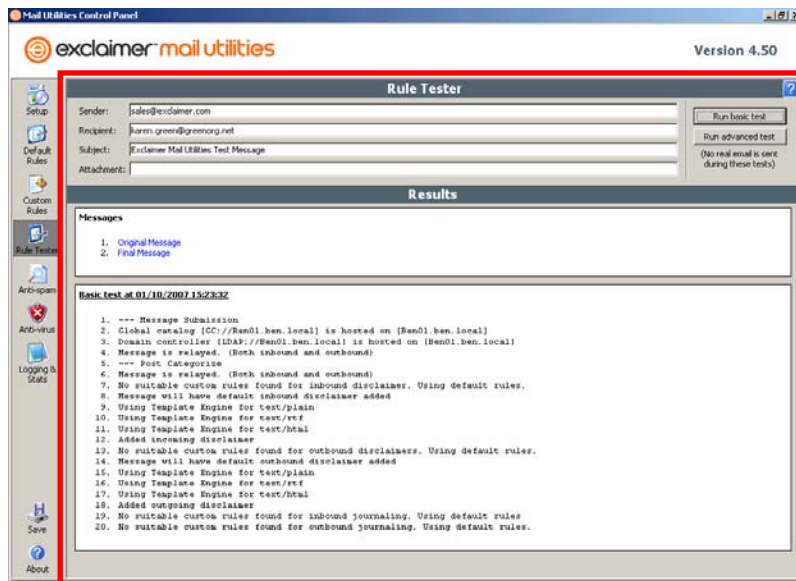
*To apply any changes you have made you must click **OK** in the Add Mail Rule box.*

*Clicking on the **Save** icon to save your settings will also*

## ▶ Rule Tester panel

### The Rule Tester panel

This is where you can test the rules you created in the Default Rules and Custom Rules panels. For example, you may want to check that a rule triggers, maybe adding a different disclaimer when an email is sent to a specific person. Please note no email messages are actually sent by Exclaimer Mail Utilities' rule tester.



#### Sender:

This is where you enter the email address of the sender of the email. This can be from a specific external domain or sent from your own internal domain.

#### Recipient:

This is where you enter the email address of the recipient of the email. This can be to a specific external domain or to a user on your own internal domain.

#### Subject:

This is where you can enter specific subjects to trigger some of your custom rules, should you have them set up in this way.

#### Attachment:

This is where you can add an attachment (as a file path e.g. 'c:\email\file1.pdf') to the email rule test.

**Run basic test**

This button displays the list of actions that will be applied to the email message. Please note no real email messages are actually sent during this test.

**Run advanced test**

This button displays a more complete list of each logical decision made by Exclaimer Mail Utilities when choosing the rules to use. This can be very useful when diagnosing why Exclaimer Mail Utilities is applying a particular rule. Please note no real email messages are actually sent during this test.

**Messages Section**

This is where you can preview the test email that you used. Clicking on the links in this section opens a dialog box that contains a preview of the email or auto-response.

**Original Message** – This represents the email message before it was sent and processed by Exclaimer Mail Utilities.

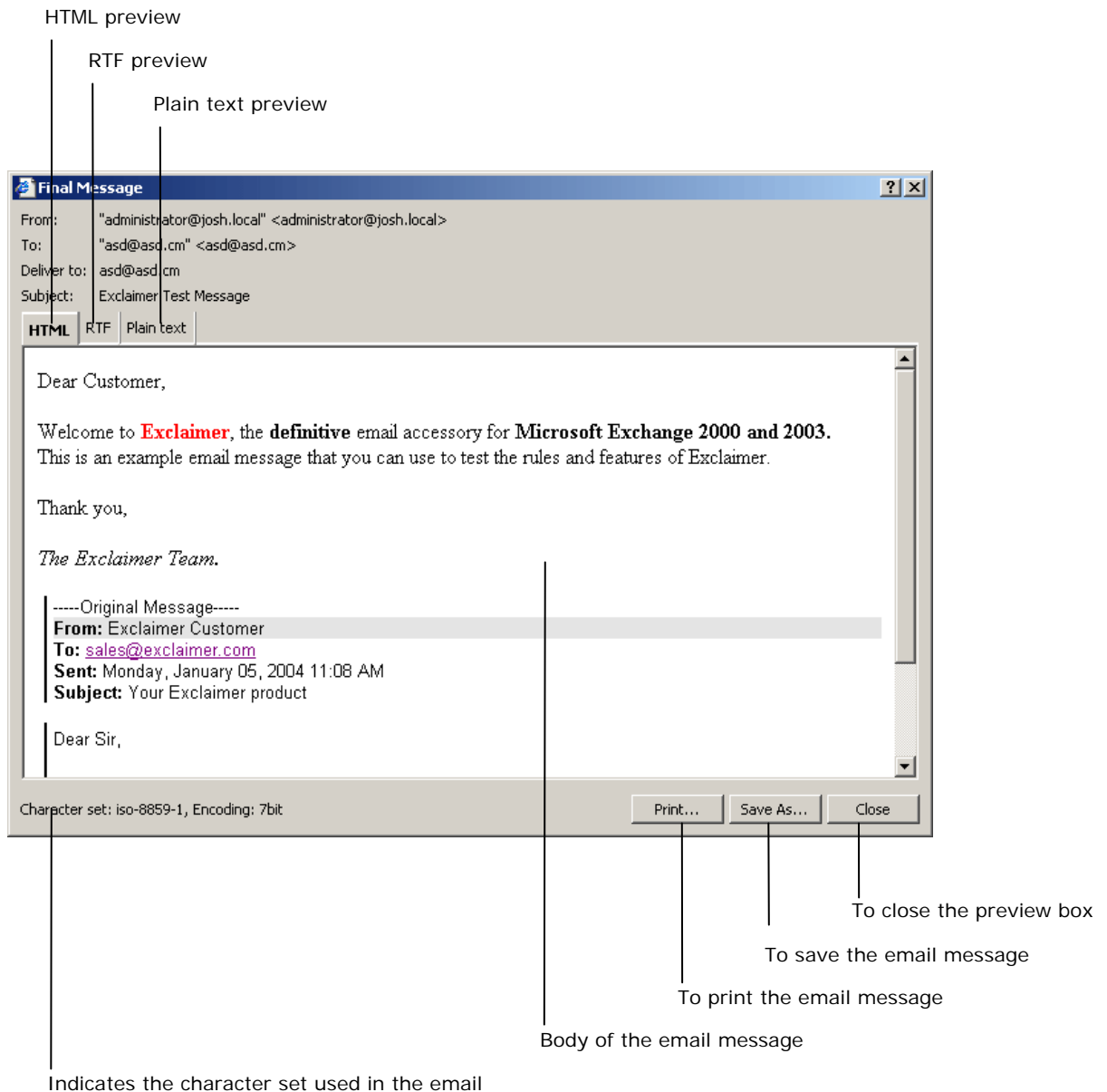
**Auto-response** - This represents the auto-response email message sent by Exclaimer Mail Utilities. This option only appears if you have an auto-responder set up.

**Journal Message** – This represents the journaled email message. This option only appears if you have selected to journal email messages.

To view the journaled email message, click on the link in the **Attachment** field of the preview box. This only applies if you have enabled envelope journaling.

**Final Message** – This represents the email message after it was processed by Exclaimer Mail Utilities and delivered.

## The preview window



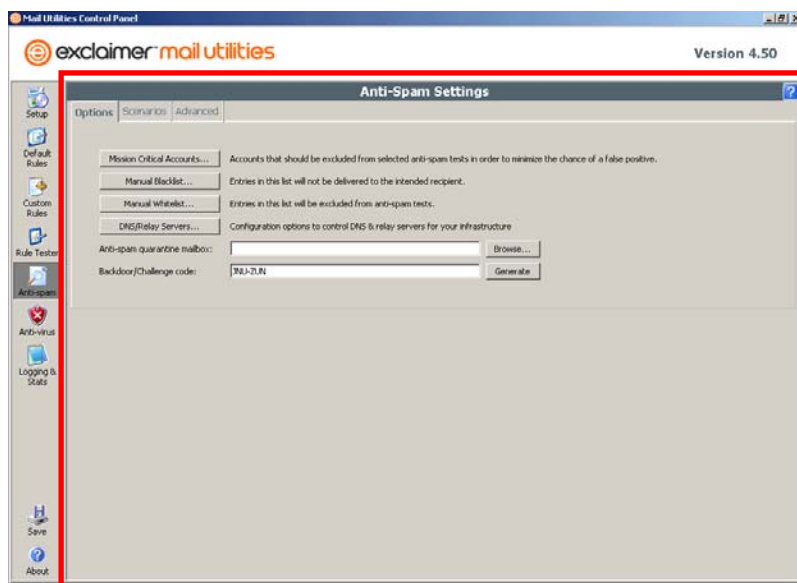
### Basic/Advanced test results box

This is where you can view the list of logical decisions Exclaimer Mail Utilities has made based on your Mail Utilities' set up (including default and custom rules) and the information that you have entered in the Rule Tester's Sender, Recipient, Subject and Attachment fields. This list will detail exactly how the test message was processed including when and what type of delivery option, disclaimer, email journaling and auto responding options have been applied to it.

## ▶ Anti-Spam Settings panel

### The Anti-Spam Settings panel

#### Options tab



**Mission Critical Accounts...** – You use this button to set up or view your organization’s mission critical accounts. These are accounts that should be excluded from selected anti-spam tests in order to minimize the possibility of false positives.

**Manual Blacklist...** – You use this button to set up or view your organization’s manual blacklist. Email addresses entered into this list will not have their email messages delivered to any recipient on your domain.

If an email address exists in both the Blacklist and the Whitelist the Blacklist entry takes priority.

**Manual Whitelist...** – You use this button to set up or view your organization’s manual whitelist. Entries in this list will be excluded from anti-spam tests.

**Anti-Spam quarantine mailbox:** – This is an optional setting where you enter the user mailbox that you want to use as your quarantine mailbox. This mailbox will contain any spam email messages you receive that Exclaimer Mail Utilities has quarantined.

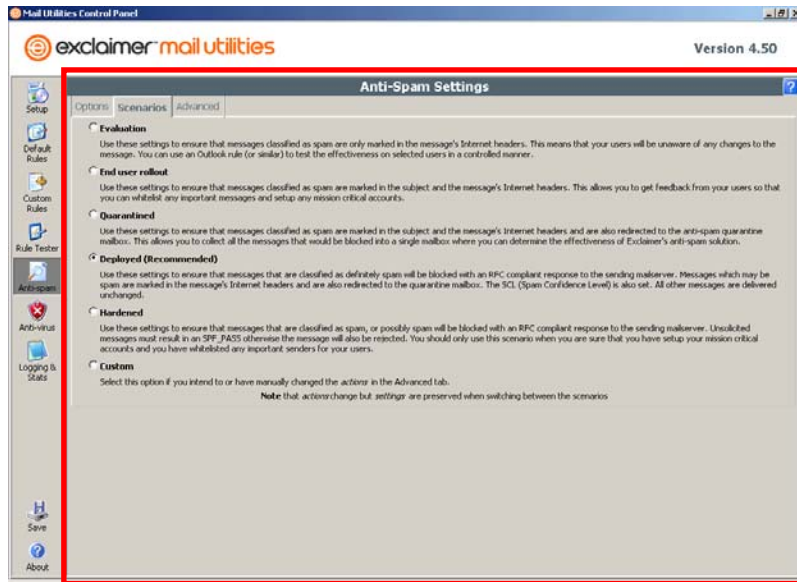
**Backdoor/Challenge code:** – This is an optional setting where you can enter a backdoor code that you would use

to allow senders of messages that had been bounced back a way of getting their message delivered.

Bounced emails are messages telling the original sender that there has been a problem delivering their email. Exclaimer Mail Utilities triggers a bounce message for email messages that resolve an SPF pass but fail other Anti-Spam tests.

The SPF pass is identified through one of Exclaimer Mail Utilities' Anti-Spam tests.

## Scenarios tab



**Evaluation** – For evaluating the effectiveness of Exclaimer’s anti-spam technology in your organisation. Emails that Exclaimer Mail Utilities identifies as spam will be marked in the mail headers so that you can prepare your own efficacy statistics whilst not outwardly modifying any of your colleagues’ emails.

**End user rollout** – For rolling out Exclaimer Mail Utilities’ anti-spam technology across your organisation. Emails that Mail Utilities identifies as Spam will be marked in the subject so that your colleagues can identify any bulk email (such as regular newsletters) that they would like to continue receiving but may be at risk of being identified as Spam. You should then use Exclaimer Mail Utilities’ great whitelisting and Auto-whitelisting technology to ensure you always receive your customers’ emails.

**Quarantined** – All messages that are classified as spam are marked in the subject field and in the message’s Internet headers. These messages are also redirected to the anti-spam quarantine mailbox. This scenario quarantines spam in a specific mailbox allowing you to assess the effectiveness of Exclaimer Mail Utilities’ Anti-Spam solution.

In order to use this option you must set up a Quarantine mailbox so that Exclaimer Mail Utilities can safely quarantine your mail.

**Deployed (Recommended)** – All emails identified by Exclaimer Mail Utilities as definitely spam are dropped. Those that may be spam are marked in the subject.

**Hardened** – Blocks all mail that is classified as spam or classified as possibly spam with an RFC compliant response to the sending mail server. Unsolicited messages must result in an SPF\_PASS otherwise the message will also be rejected.

Only use this scenario when you are sure that you have setup your mission critical accounts and you have whitelisted any important senders for your users.

**Custom** – Use this option only if you intend to manually change the actions in the **Advanced** tab.

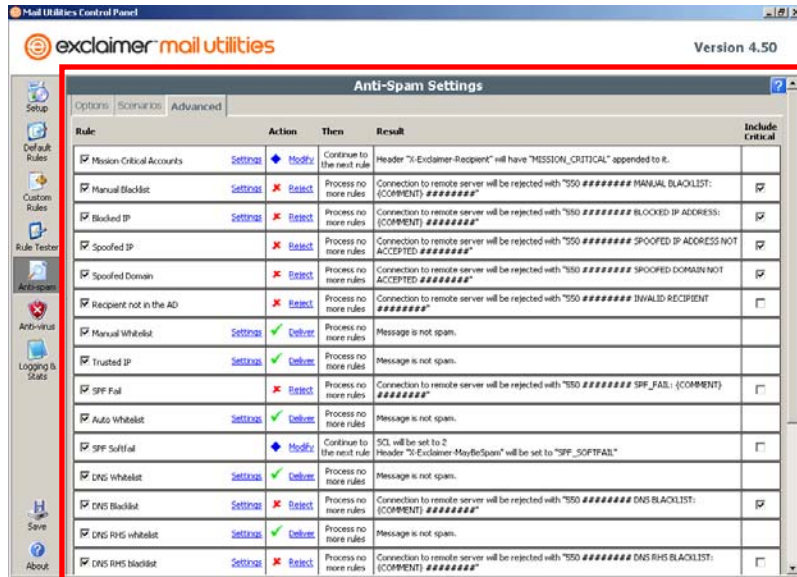
**IMPORTANT!**

*You are **STRONGLY ADVISED** not to evaluate Exclaimer Mail Utilities' anti-spam technology in a lab environment. Exclaimer Mail Utilities does not use content to identify spam. Instead, its combination of spoofing detection, blacklisting and outbreak detection means that you must arrange for a genuine combination of legitimate email and spam to be processed by Exclaimer Mail Utilities to establish its efficacy.*

***Note** – email messages are only bounced if they resolve an SPF pass but fail other Anti-Spam tests. Senders who receive a bounce message can follow a simple set of instructions on how they can successfully resend their message.*

## Advanced tab

This tab contains all the Anti-Spam tests Exclaimer Mail Utilities performs on all incoming email messages. These settings allow you to customize your Anti-Spam setting to your exact requirements. However, you do not need to adjust these settings as Exclaimer Mail Utilities has a selection of preset Anti-Spam settings for you to choose from. See the *Scenarios tab* topic on the previous page.



## Key:

- No more tests are triggered and the email message is categorized.
- ◆ Passes email message on to the next test
- ✓ Delivers the email message
- ✗ Rejects the email message

The table is divided up into five columns:

**Rule** – Contains the names of each individual spam test.

**Action** – This determines what each test does when it is triggered.

**Then** – This details what the test does once it has completed its process.

**Result** – This details what happens to a message if it matches the test criteria.

**Include Critical** – When left unchecked, messages to mission critical accounts will be excluded from the Anti-Spam tests.

The spam tests that are performed on all incoming email messages are as follows:

**Mission Critical Accounts** – Mission critical accounts provide a way to bypass some or all of the other anti-spam tests for accounts that are more important than others. This might be 'sales@...' address if you are worried about false positives. These Mission Critical Accounts can be specified by AD User, Group, Contact or SMTP address.

Obviously the reduced level of anti-spam checking means that these accounts will always get more spam than ones that are not mission critical, although you can control exactly which future tests are pertinent to mission critical accounts.

*The earliest point that this can be classified by Exclaimer Mail Utilities is at the RCPT TO: phase.*

**Manual Blacklist** – Manual blacklist provides a way to block messages based on combinations of details ranging from IP address through to envelope sender/recipient, message sender/recipients and even subject content.

This is a very powerful way to block messages that are not caught by other anti-spam tests. It can be used to help enforce compliance issues, such as preventing non-spammers from harassing employees.

*The earliest point that this can be classified by Exclaimer Mail Utilities depends upon the data that is present in the blacklist test.*

*If only IP address is specified, then this classification can happen at HELO/EHLO and then all other messages transmitted during this session will have at least this classification.*

*If Envelope FROM is specified then the earliest this classification can happen is at MAIL FROM:*

*If Envelope TO is specified then the earliest this classification can happen is at RCPT TO:*

*All other details require the message to be classified after the DATA command is complete.*

**Blocked IP** – Blocked IP is similar to Manual Blacklist, but it offers the ability to block whole chunks of the internet. For instance, you might decide that you don't want to receive email from some particular ISP or country.

IP addresses are (loosely) broken up in to geographic units (at least at the larger levels), and within those, ISPs are allocated blocks of addresses.

It is possible to specify a range of addresses using the CIDR notation, e.g. 10.0.0.0/8 would be a range of 16777216 IP addresses from 10.0.0.0 thru 10.255.255.255.

*The earliest point that Blocked IP can be classified is at HELO/EHLO.*

**Spoofed IP** – Spoofed IP is when a sending mail server signs on in the HELO phase with an IP address as the HELO parameter that is not the same as its connection IP address.

Since this is such a trivial check to make, it's a wonder that this technique is ever used.

No legitimate email servers ever do this, and it's normally a virus Trojan trying to replicate itself to your system. This classification should always result in a rejected or quarantined message.

*The earliest point that Spoofed IP can be classified is at HELO/EHLO.*

**Spoofed Domain** – This classification is similar to Spoofed IP. This is where the sending mail server pretends that it's one of the domains that you are authoritative for in the HELO command.

It's a bit like someone ringing you and when you pick up the phone to answer and they say "Hello, it's George". Well, you know it's not George, because that's you.

*The earliest point that Spoofed Domain can be checked is HELO/EHLO.*

**Recipient not in the AD** – Recipient not in the AD is just as it sounds. It's a test designed to filter out messages to people who don't exist, and you'd be surprised at just how many of them there are.

Obviously email classified as such would not normally constitute a problem for you since no one would ever see this email, but if your systems issue an NDR then some unsuspecting person may end up with a message telling them that they had sent a message that they hadn't.

There is a caveat to this test, which is if any of the recipients on the message are real, then this classification is not performed. For example, a message to a single person who is not in your AD will result in this test triggering as will a message to other non-existent people all of whom are not in the AD. If there is a single recipient who is in the AD, then this test will not trigger. Don't worry though, there are plenty of opportunities to catch this message if it is a spam one later.

*The earliest point that Recipient not in AD can be checked is at RCPT:*

**Manual Whitelist** – Manual Whitelist is similar in nature to the Manual Blacklist. You can use this to ensure that messages from certain sources, people or containing a certain combination of text characters in the subject are excluded from further anti-spam tests.

*The earliest point that this can be classified by Exclaimer Mail Utilities depends upon the data that is present in the Whitelist test.*

*If only IP address is specified, then this classification can happen at HELO/EHLO and then all other messages transmitted during this session will have at least this classification.*

*If Envelope FROM is specified then the earliest this classification can happen is at MAIL FROM:*

*If Envelope TO is specified then the earliest this classification can happen is at RCPT TO:*

*All other details require the message to be classified after the DATA command is complete.*

**Trusted IP** – Trusted IP is a server that you know will never generate spam. This is usually a web server or other automatic system under your administrative control that can generate email messages.

You simply add the IP address (or subnet) of the machine that you are confident will never send spam.

*The earliest point that this classification can occur is at HELO/EHLO.*

**SPF Fail** – The SPF fail test is when the connecting mail server attempts to deliver messages from a particular domain and the SPF policy (stored in DNS) indicates that the connection mail server's IP address is not acceptable.

SPF is intended to protect the domain and is checked by receiving mail servers. There are many systems on many different platforms that now check SPF policy and it is a great way to reject out-and-out spoofed domains and gives some credibility to those that pass.

Generally speaking mail servers that fail the SPF policy are subject to being rejected by many large ISPs and many mail server implementations.

*The earliest point that this classification can be performed is at MAIL FROM:*

For more information on RFC standards visit <http://www.rfc-editor.org/>.

**Auto Whitelist** – The Auto Whitelist is a list of smtp addresses generated by Exclaimer Mail Utilities of all the recipients of outbound messages.

This means that anyone you send email to will be able to reply without triggering most of the anti-spam tests. Obviously if they trigger any of the tests before this one, then they are subject to being classified differently.

Exclaimer Mail Utilities comes with a wizard to enable a rapid setup of this file, and this will scan your entire Exchange organization extracting the smtp addresses of all the people you have sent email to or received email from. Deleted Items and Junk mail are obviously excluded from this scan.

Once this wizard has completed, Exclaimer Mail Utilities will have a large database of all the people you regularly communicate with and this allows you to have a high degree of confidence that you won't miss an important email because of a misclassification.

There is a practical limit to the size that this list can become and we've defaulted this to 50,000 entries.

Old (stale) entries are removed in the natural course of time – correspondents that you communicate regularly with have their importance increased so that they are less likely to “fall off the end”.

*The earliest point that this classification can be performed is at MAIL FROM:*

**SPF Softfail** – This test is similar to SPF fail, but is not as aggressive. It merely indicates that the domain owner was unsure if the sending mail server was legitimate or not. The SPF specification states that email with this classification may be treated to more scrutiny.

You can choose to reject messages of this classification if you so wish.

*Like the SPF Fail, the earliest point that this classification can be performed is MAIL FROM:*

**DNS Whitelist** – DNS Whitelists are not as successful as once hoped, but there is good reason for an optimistic future. The theory is that if your IP address has a reputation for not sending spam, then you might be able to bypass irritating content based anti-spam systems.

This primarily targets large bulk mail senders and has so far not shown an ability to deal with legitimate mail list servers. This situation is sure to change over time which is the reasoning behind this classification.

*The earliest point that this can be performed is at HELO/EHLO.*

**DNS Blacklist** – Exclaimer Mail Utilities relies primarily on Spamhaus, who in our opinion operate one of the most professional services on the internet. We also refer to SpamCop, NJABL and SORB all of whom offer credible services albeit slightly more aggressive.

All of these organizations maintain lists of IP addresses that have sent or are currently in the process of sending spam. Some of them also maintain lists of dial-up address ranges and other machines that their subscribers would not like to communicate with.

Some of these DNS Blacklists are used to reject email from certain servers outright while others verify and classify email as bulk.

*The earliest point that this classification can be performed is at HELO/EHLO.*

**DNS RHS Whitelist** – Where the DNS Whitelist classification is attempting to check the IP address of the incoming mail server, the RHS variation checks the domain of the sender for his reputation.

Again, there is very little available in this category at the present.

*The earliest point that that this classification can be performed is at MAIL FROM:*

**DNS RHS Blacklist** – DNS RHS Blacklists only provide a way to trap a small amount of spam. The service provider that we use is bogusmx at <http://www.rfc-ignorant.org/>. This is a list of domains that have been proven to use bogus MX records.

This was once a way for a spammer to bypass naïve checks that the sending domain had an MX record in DNS without actually having to have a mail server.

*The earliest point that this classification can be performed is at MAIL FROM:*

**Detection Center** – The Detection Center monitors spam outbreaks and trends, and classifies the messages accordingly. In order to reach their target audience spammers have to operate campaigns with hundreds of millions of messages. This kind of activity has a consequence especially when looking at patterns of email traffic over the world. You can observe our real time monitor on the website [www.exclaimer.com/antispamoutbreakmonitor.aspx](http://www.exclaimer.com/antispamoutbreakmonitor.aspx) and see outbreaks happening in real-time.

The Detection Center will classify messages as Spam, Bulk or Not Spam. We further sub-classify the Bulk messages by also referring back to the more aggressive DNS Blacklists and we also check the sending domain to see if it passes the domain SPF policy.

*The earliest point that these classifications can be performed is after the DATA command is complete.*

**Detection Center – Bulk (SPF\_PASS)** – Messages that are confirmed bulk (and are not sent from servers that appear in the more aggressive DNS Blacklists) where the domain sending them has an SPF policy that results in a PASS will have this classification.

This is normally a 'white' classification since the sender has had to go to considerable effort to get this message delivered. For example, being checked against no less than 4 public anti-spam list providers and being classified as a bulk email sender.

**Detection Center – Bulk** - Bulk messages are still checked with the more aggressive DNS Blacklists which (if needed) will override the bulk classification.

**Detection Center – Spam** - The message is part of an ongoing spam outbreak.

**SPF PASS** – Messages that result in an SPF pass will be classified with this test. This allows for a very aggressive stance to be taken, for example, you can choose not to accept unsolicited messages from domains that do not result in an SPF pass.

This kind of aggressive stance on email messages should only be taken with the full knowledge that you will only receive messages that are sent from servers that result in an SPF PASS.

However, this test does not guarantee that a message is not spam, it merely ensures that there is a high degree of probability that the sender of this message is; a) genuine, b) sent the message and, c) can deal with the spam problem if that is what it is.

*The earliest point that this classification can be performed is at MAIL FROM:*

**HTML Emails** – Exclaimer Mail Utilities does not have a scenario that uses this classification; however, it can be useful for very aggressive mail administrators who do not want to permit HTML email unless the sender is white listed.

This may seem quite tough but it can deal with a large portion of spam that comes in this form.

*The earliest point that this classification can be performed is after the DATA phase.*

**Email with attachment** – Exclaimer Mail Utilities does not have a scenario that uses this classification; it can be useful for very aggressive mail administrators who do not want to permit email that has attachments unless the sender is white listed.

This may seem quite tough, but it can deal with a large portion of spam that comes in this form.

*The earliest point that this classification can be performed is after the DATA phase.*

**Unclassified** – Messages that have remained unclassified through all the previous white and black testing will have this classification.

This classification could be used to implement a 'challenge-response' type solution.

Challenge-Response on its own is generally regarded as a bad technique to combat spam. Nevertheless, it is a very effective solution and this is what initially attracts people to it. This kind of approach is generally considered bad practice because the backscatter generated from challenging every spam message simply adds to the problem on the internet rather than reducing it.

However, if you choose to implement a challenge-response approach then we recommend you use as many of the previous tests to classify the message in other ways before issuing a challenge.

This is the premise behind the 'Hardened' scenario where messages that are not classified as spam or not-spam that do not result in SPF pass are issued a challenge.

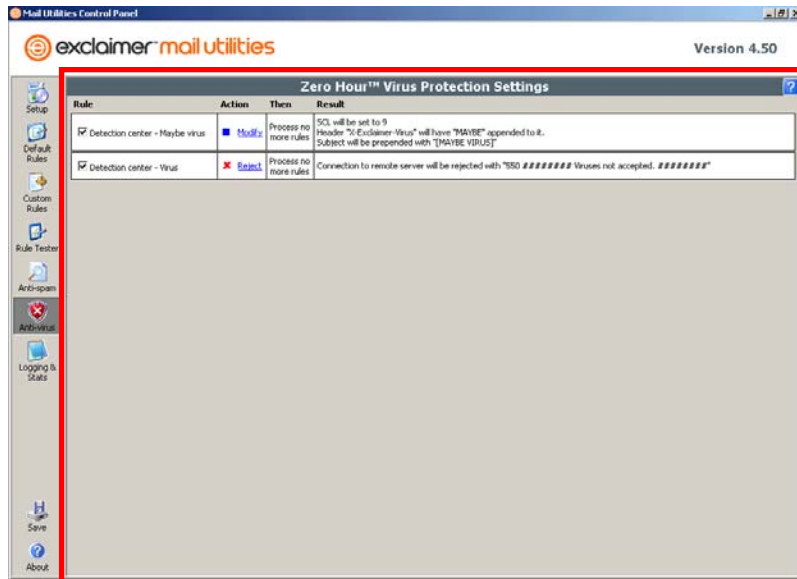
**IMPORTANT!**

*It is quite permissible to start with a pre-defined scenario and then make custom changes to that scenario.*

*To apply any changes you have made you must click on the **Save** icon in the left-hand menu.*

## ▶ Anti-Virus Settings panel

### The Anti-Virus Settings panel



This panel contains all the Anti-Virus tests Exclaimer Mail Utilities performs on all incoming email messages. The table is divided up into four columns:

**Rule** – Contains the names of each individual virus test.

**Action** – This determines what each test does when it is triggered.

**Then** – This details what the test does once it has completed its process.

**Result** – This details what happens to a message if it matches the test criteria.

The virus tests that are performed on all incoming email messages are as follows:

**Detection center – Maybe virus** – This identifies email messages that are suspected of containing a virus.

**Detection center – Virus** – This rejects email messages that contain a virus.

***IMPORTANT!***

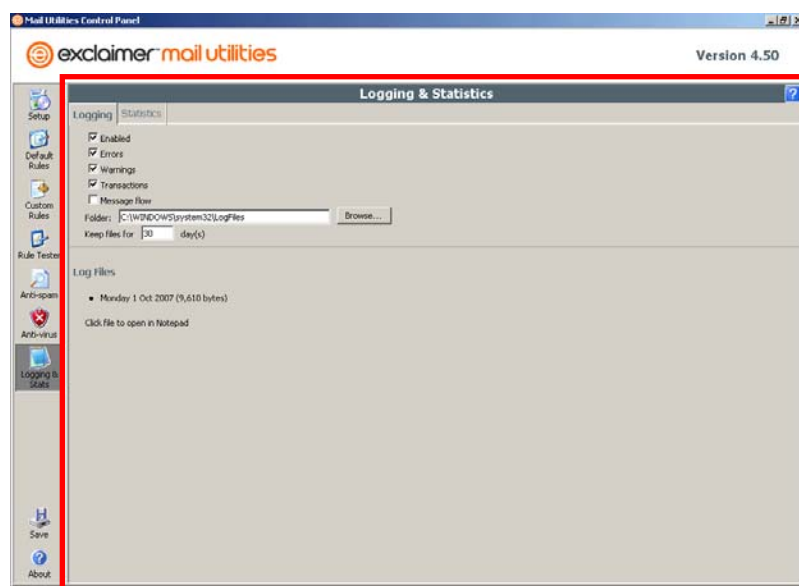
*To apply any changes you have made you must click on the **Save** icon in the left-hand menu.*

## ▶ Logging & Stats panel

### The Logging & Statistics panel

This panel is broken down into two tabs that contain data on Exclaimer Mail Utilities' performance and settings.

#### Logging tab



**Enabled** – To enable or disable Exclaimer Mail Utilities' error, warnings, transaction and message flow logging. You need to place a tick in this checkbox before you can enable the options below.

**Errors** – Place a tick in this checkbox to enable Exclaimer Mail Utilities' error logging.

**Warnings** – Place a tick in this checkbox to enable Exclaimer Mail Utilities' warning logging.

**Transactions** – Place a tick in this checkbox to enable Exclaimer transaction logging.

**Message flow** – Place a tick in this checkbox to enable Exclaimer Mail Utilities' message flow logging.

**Folder:** – You use this to enter the root of the folder where you want Exclaimer Mail Utilities' log files to be saved.

**Keep files for** – You use this to enter the number of days you want to keep the Exclaimer Mail Utilities' log file for.

Once the age of a log file has exceeded the number of days you specify it will be permanently deleted.

**Log Files** – This contains a list of all the log files Exclaimer Mail Utilities has created. To view a log you simply click on it. Exclaimer's log files are saved as text files (.txt) and usually open in **Notepad**.

## Statistics tab

| Emails Processed |   |
|------------------|---|
| Incoming         | 2 |
| Internal         | 0 |
| Outgoing         | 2 |
| Total            | 2 |

| Features                             |        |
|--------------------------------------|--------|
| Up time                              | 0 secs |
| Disclaimers - Incoming               | 2      |
| Disclaimers - Internal               | 0      |
| Disclaimers - Outgoing               | 2      |
| Disclaimers - Total                  | 4      |
| Journalled incoming messages         | 0      |
| Journalled internal messages         | 0      |
| Journalled outgoing messages         | 0      |
| Journalled messages                  | 0      |
| Delivery Options                     | 0      |
| Autoreponse                          | 0      |
| Anti-spam: Not Spam                  | 0      |
| Anti-spam: Marked                    | 0      |
| Anti-spam: Rejected                  | 0      |
| Anti-spam: Bounced                   | 0      |
| Anti-spam: Discarded                 | 0      |
| Anti-spam: Detection center messages | 0      |
| Anti-spam: Auto-Whitelist size       | 0      |

| Errors & Warnings                    |   |
|--------------------------------------|---|
| Feature Failed - Incoming disclaimer | 0 |
| Feature Failed - Internal disclaimer | 0 |
| Feature Failed - Outgoing disclaimer | 0 |
| Feature Failed - Journalled message  | 0 |
| Feature Failed - Delivery Options    | 0 |
| Feature Failed - Auto responder      | 0 |
| Auth Tolerance Triggered             | 0 |

This tab is broken down into eight sections:

**Exclaimer Emails Processed** – This section counts the number of incoming, internal and external email messages that have been received or sent.

**Incoming** Number of messages classified as incoming that have been received by Exclaimer Mail Utilities. This does not include any messages that may have been dropped or aborted because of anti-spam classifications.

**Internal** Number of messages classified as internal.

**Outgoing** Number of messages classified as outgoing.

**Total** Total number of messages received by Exclaimer Mail Utilities. This number may be larger than the sum of the previous three counters because certain types of messages are excluded from any further analysis. These are:

- Administrative messages that were from the Exclaimer system
- Read-receipt (or other messages) messages from mail monitor accounts

If all the Exclaimer Mail Utilities' features are disabled then this counter will still increment but none of the classified counters will.

**Exclaimer Features** – This section counts the number of email messages that pass through certain Exclaimer Mail Utilities' features. For example, you can count the number of email messages that have had disclaimers added to them.

**Up time** Time in weeks, days, hours, minutes and seconds that the Exclaimer Mail Utilities' system has been running. Each time the server is rebooted or the IIS admin service is restarted, this counter will reset.

**Disclaimers - Incoming** Number of messages that were classified as incoming that had a successful disclaimer added.

**Disclaimers - Internal** Number of messages that were classified as internal that had a successful disclaimer added.

**Disclaimers - Outgoing** Number of messages that were classified as outgoing that had a successful disclaimer added.

**Disclaimers - Total** Total number of disclaimers that were added to messages.

**Journalled incoming messages** Number of messages that were classified as incoming that were journalled

|   |  |
|---|--|
| <b>Journalled internal messages</b>         | Number of messages that were classified as internal that were journalled   |
| <b>Journalled outgoing messages</b>         | Number of messages that were classified as outgoing that were journalled   |
| <b>Journalled messages</b>                  | Total number of messages that were journalled  |
| <b>Delivery Options</b>                     | Total number of messages that had delivery options applied to them   |
| <b>Auto response</b>                        | Total number of messages that triggered an auto-response.  |
| <b>Anti-spam: Not Spam</b>                  | Total number of messages that were classified as incoming that were set to deliver directly without any further anti-spam tests.   |
| <b>Anti-spam: Marked</b>                    | Total number of messages that were classified as incoming that were marked in some way by the anti-spam tests.   |
| <b>Anti-Spam: Rejected</b>                  | Total number of messages that were classified as incoming and rejected during the SMTP protocol by Exclaimer's Anti-spam engine.   |
| <b>Anti-Spam: Bounced</b>                   | Total number of bounce messages sent. A Bounce message is generated by Exclaimer Mail Utilities' Anti-Spam engine when an email has resolved an SPF pass but fails to pass other Anti-Spam tests.                    |
| <b>Anti-spam: Discarded</b>                 | Total number of messages that were classified as incoming and dropped during the SMTP protocol or were aborted during transport because they were classified as spam and the anti-spam settings were set to "Reject" |
| <b>Anti-spam: Detection center messages</b> | Total number of messages that were classified as incoming and submitted to the detection center for analysis.  |

**Anti-spam:** Total number of email addresses in the automatic whitelist.  
**Auto-Whitelist size**

**Exclaimer Errors & Warnings** – This section counts the number of errors and warnings where Exclaimer Mail Utilities has encountered a problem. For example, the number of incoming email messages where Exclaimer Mail Utilities has failed to add a disclaimer.

**Feature Failed - Incoming disclaimer** - Total number of messages that should have had an incoming disclaimer added but failed to do so.

**Feature Failed - Internal disclaimer** - Total number of messages that should have had an internal disclaimer added but failed to do so.

**Feature Failed - Outgoing disclaimer** - Total number of messages that should have had an outgoing disclaimer added but failed to do so.

**Feature Failed - Journalled message** - Total number of messages that should have been journalled but failed to do so.

**Feature Failed - Delivery Options** - Total number of messages that should have triggered a delivery option but failed to do so.

**Feature Failed - Autoresponder** - Total number of messages that should have triggered an auto-responder but failed to do so.

**Fault Tolerance Triggered** - Total number of failures that triggered the error handling/fault tolerance action in Exclaimer Mail Utilities.

**Detection Center Faults** - Total number of faults reported by the anti-spam detection center.

**Exclaimer Spam Engine Counters** – This section counts the number of email messages that have triggered each spam test. For example, if an email message is received where the recipient is not in the Active Directory the **Recipient Not in AD** count will increase by 1.

|                            |   |
|----------------------------|---|
| <b>Mission Critical</b>    | Total number of messages that were not spam checked because the recipient was a mission critical account. |
| <b>Recipient Not in AD</b> | Total number of messages that were to unknown recipients.   |
| <b>Auto-Whitelisted</b>    | Total number of messages that were not spam checked because the sender was in the automatic whitelist.    |
| <b>Trusted IP</b>          | Total number of messages that were classified as having a trusted IP address.                             |
| <b>Blocked IP</b>          | Total number of messages that were classified as having a blocked IP address.                             |
| <b>Spoofed IP</b>          | Total number of messages that were classified as having a spoofed IP address.                             |
| <b>Spoofed Domain</b>      | Total number of messages that were classified as having a spoofed domain in the HELO command.             |
| <b>SPF FAIL</b>            | Total number of messages that were classified as failing the SPF checks.                                  |
| <b>SPF SOFTFAIL</b>        | Total number of messages that were classified as softfailing the SPF checks.                              |
| <b>DNS WL</b>              | Total number of messages that were classified using a DNS whitelist.                                      |
| <b>DNS BL</b>              | Total number of messages that were classified using a DNS blacklist.                                      |
| <b>DNS RHS WL</b>          | Total number of messages that were classified using a DNS domain whitelist.                               |
| <b>DNS RHS BL</b>          | Total number of messages that were classified using a DNS domain blacklist.                               |
| <b>Local Whitelist</b>     | Total number of messages that were classified in the local whitelist.                                     |

**Local Blacklist** Total number of messages that were classified in the local blacklist.

**Detection Center Bulk (With SPF\_PASS)** Total number of messages that were classified by the detection center as BULK where the domain resulted in SPF\_PASS.

**Detection Center Bulk** Total number of messages that were classified as BULK by the detection center.

**Detection Center Spam** Total number of messages that were classified as SPAM by the detection center.

**SPF PASS** Total number of messages that were classified as passing the SPF checks.

**HTML Email** Total number of messages that were HTML formatted.

**Email with attachment** Total number of messages that had attachments.

**Unclassified** Total number of messages that were unclassified.

**Exclaimer Virus Engine Counters** – This section counts the number of email messages that have triggered each virus test. For example, each time a virus infected email message is detected by Exclaimer Mail Utilities the **Detection Center Virus** count will increase by 1.

**Detection Center Maybe Virus** Total number of messages that were classified as maybe virus by the detection center.

**Detection Center Virus** Total number of messages that were classified as virus by the detection center.

**Exclaimer Timings** – This section monitors the amount of time it takes Exclaimer Mail Utilities to process certain features. For example, the amount of time it takes to add a disclaimer to an email message.

The counters in the timings and throughput sections have extra data computed by the Exclaimer Mail Utilities' UI which is not available in the Perfmon counters as this information cannot be computed using the Perfmon tool. Exclaimer Mail Utilities monitors the min, max, total and average values for the following counters.

The timing counters all show elapsed time, not processor time. This means that the timer was started when Exclaimer Mail Utilities started the operation in question and was stopped when the operation completed. In a multi-tasking, distributed system these numbers can be substantially altered by the environment; how many processes/threads running on the local system, network performance, connectivity issues, catalog/domain controller performance.

|                              |   |
|------------------------------|---|
| <b>Open Directory (ms)</b>   | Elapsed time in milliseconds taken to open a catalog server or domain controller for a query for categorization or rule processing. This counter is unused in versions of Exclaimer Mail Utilities prior to 4.10. |
| <b>Categorize (ms)</b>       | Elapsed time in milliseconds taken to categorize the sender and recipients of a message to determine if they are incoming, internal or outgoing and to collect any other data from catalog servers for them.      |
| <b>Rule Lookup (ms)</b>      | Elapsed time in milliseconds taken to find custom rules.  |
| <b>Add Disclaimer (ms)</b>   | Elapsed time in milliseconds taken to add disclaimers.  |
| <b>Journaling (ms)</b>       | Elapsed time in milliseconds taken to journal messages.   |
| <b>Delivery Options (ms)</b> | Elapsed time in milliseconds taken to process delivery options.   |
| <b>Auto-responder (ms)</b>   | Elapsed time in milliseconds taken to process auto-responders.  |
| <b>Save (ms)</b>             | Elapsed time in milliseconds taken to save the message to the backing store (Exchange or Filesystem) after a modification such as adding a disclaimer has occurred.   |

|                                     |   |
|-------------------------------------|---|
| <b>Spam Check (ms)</b>              | Elapsed time in milliseconds taken to check incoming messages for spam.                                     |
| <b>DNS Lookup (ms)</b>              | Elapsed time in milliseconds taken waiting for DNS servers to reply for anti-spam operations.               |
| <b>Detection center lookup (ms)</b> | Elapsed time in milliseconds taken for the round trip to the detection center for anti-spam classification. |
| <b>Total (ms)</b>                   | Elapsed time in milliseconds that Exclaimer Mail Utilities was processing messages.                         |

**Exclaimer Throughput** – This section monitors the amount of time it takes for Exclaimer Mail Utilities to process and categorize email messages.

|                                       |   |
|---------------------------------------|---|
| <b>Message Submission - In / sec</b>  | Total number of messages per second being received by Exclaimer Mail Utilities at the message submission stage.   |
| <b>Message Submission - Out / sec</b> | Total number of messages per second leaving Exclaimer Mail Utilities at the message submission stage. If the total number In/sec is greater than the total number Out/sec then this may indicate a message flow problem. Investigation of any errors being generated is recommended.    |
| <b>Post Categorize - In / sec</b>     | Total number of messages per second being received by Exclaimer Mail Utilities at the post categorization stage.  |
| <b>Post Categorize - Out / sec</b>    | Total number of messages per second leaving Exclaimer Mail Utilities at the Post Categorize – Out stage. If the total number In/sec is greater than the total number Out/sec then this may indicate a message flow problem. Investigation of any errors being generated is recommended. |
| <b>Size (MB)</b>                      | Total size of messages being sent through Exclaimer Mail Utilities. This number includes messages with attachments.   |

**Exclaimer DLL** – This section monitors the demands that email traffic puts on Exclaimer Mail Utilities and the Server's processes.

**Sinks loaded** Number of sinks loaded at the current moment in time. A sink is a unit of code that is used by Windows SMTP service or Microsoft Exchange to provide 3rd party functionality in the mail transport flow. The number of sinks is typically between 6-10. If the number of sinks is substantially more than this, there may be a problem on your mail server.

**Processes** Each process that loads the exclaimer.DLL is counted here. This number should never show zero as any tool that can read this number should implicitly load the DLL. This counter may be useful during uninstall when it is necessary to ensure that there are no processes holding the DLL open. For more information visit the Exclaimer Knowledge Base <http://forums.exclaimer.com/forums/21/ShowForum.aspx>.

**Threads** The total number of threads that Exclaimer Mail Utilities has started for processing. This includes all active and all waiting threads

**Active threads** The total number of active threads that are currently processing messages in the Exclaimer Mail Utilities' environment. This number will normally reflect how busy the server is at any particular time.

**Queued Log Lines** Number of lines that are queued for lazy write to the log file. If this is a large number, this may indicate a problem (perhaps low disk space) in the log file directory.

**Queued Messages** Number of messages passed to Exclaimer that have not been processed yet.

**Reset Stats** – This button resets all the counters and monitoring devices to 0.

**Refresh Stats** – This button refreshes all the stats so you can view the most up-to-date information.

**Copy** – This button copies all the statistics to the clipboard where you can paste it into another program like Notepad.

**IMPORTANT!**

*We recommend that you enable **Errors and Warnings**. This way, errors during Exclaimer Mail Utilities' operation will be logged which may help any Exclaimer Technical Support investigation.*

*The statistics panel refreshes every 10 seconds.*

*If you have made any changes in the logging panel you can apply any changes you have made by clicking on the **Save** icon in the left-hand menu.*

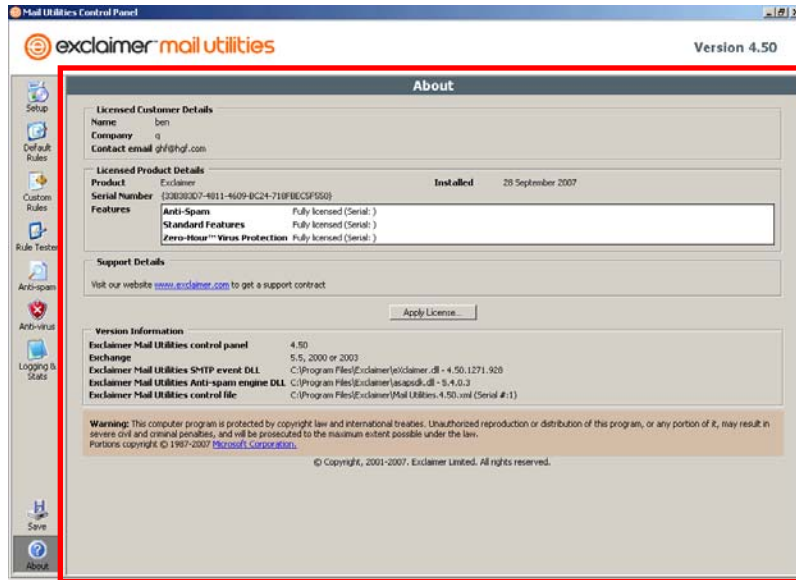
*All these statistics are available as PerfMon counters.*

*The statistics in the **Statistics** tab will be reset when you reboot your server.*

## ► About panel

### The About panel

This panel contains information concerning the licensing and version of the Exclaimer Mail Utilities software. This is also where you apply your Exclaimer license and activate the software



#### Licensed Customer Details

Contains the details of the customer this version of Exclaimer Mail Utilities is licensed to.

#### Licensed Product Details

Contains the features that are licensed on the product, the license serial number, the date the product was installed and (if a trial version) how many days are remaining on the license.

#### Support Details

Contains the number of days remaining on your support subscription and a link to our website where you can find support information.

#### Version Information

Contains exact versions of specific Exclaimer Mail Utilities' components for diagnostic and fault rectification purposes.

## Applying a license

To apply your Exclaimer Mail Utilities' license click on the **Apply License...** button and follow the instructions in the Apply License box.

# Appendix A

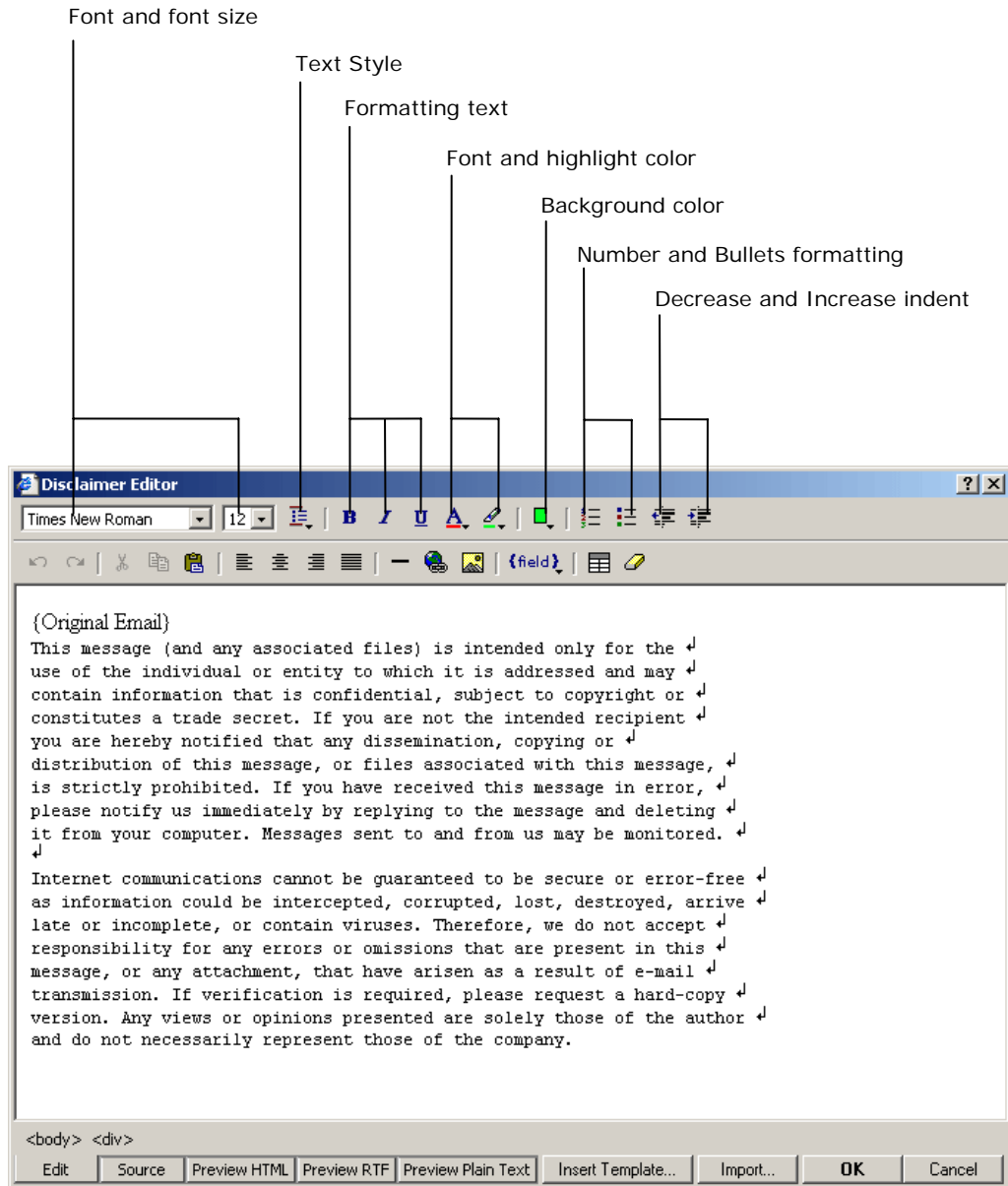
## Exclaimer Mail Utilities – Other tools and features

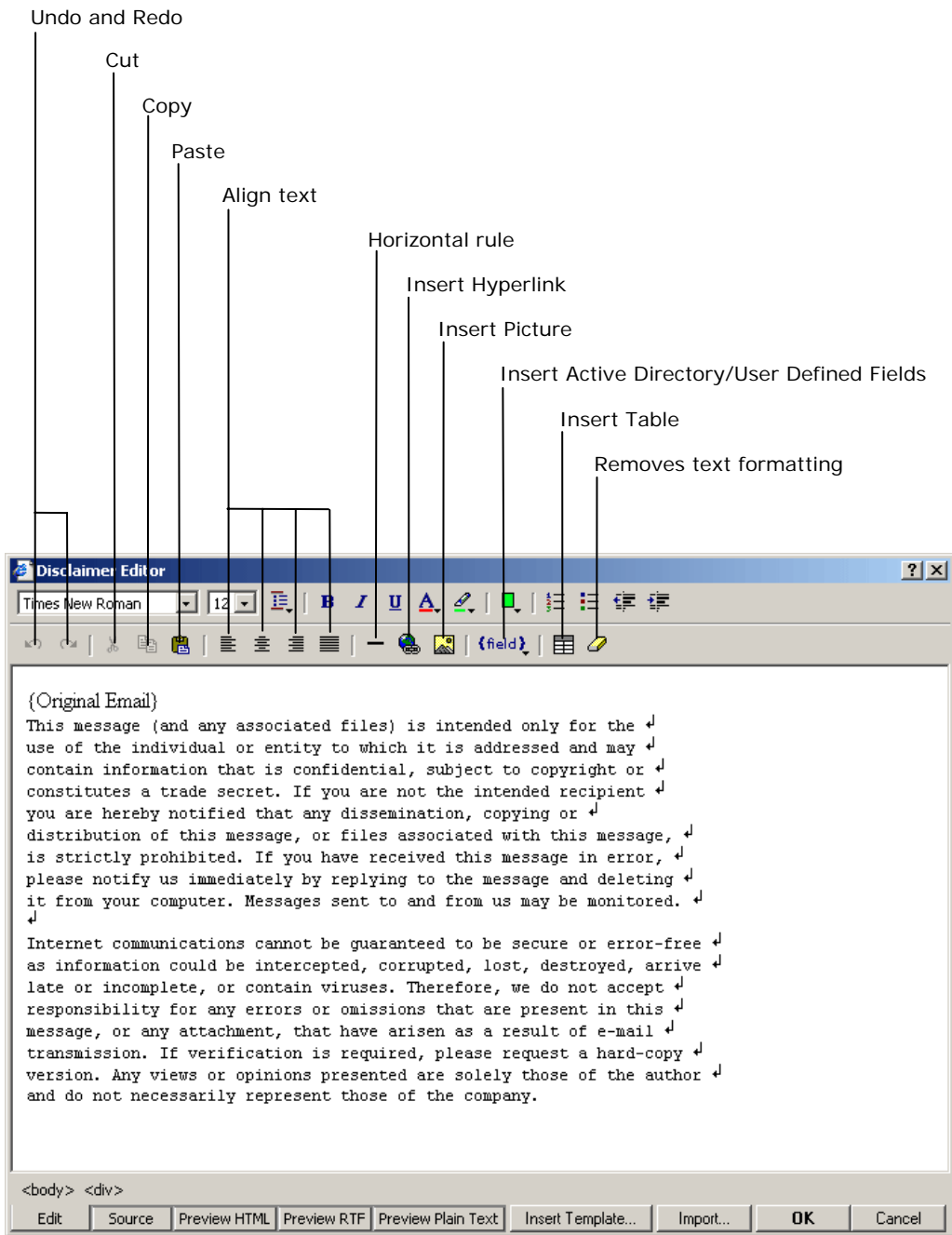
## ► Disclaimer Editor

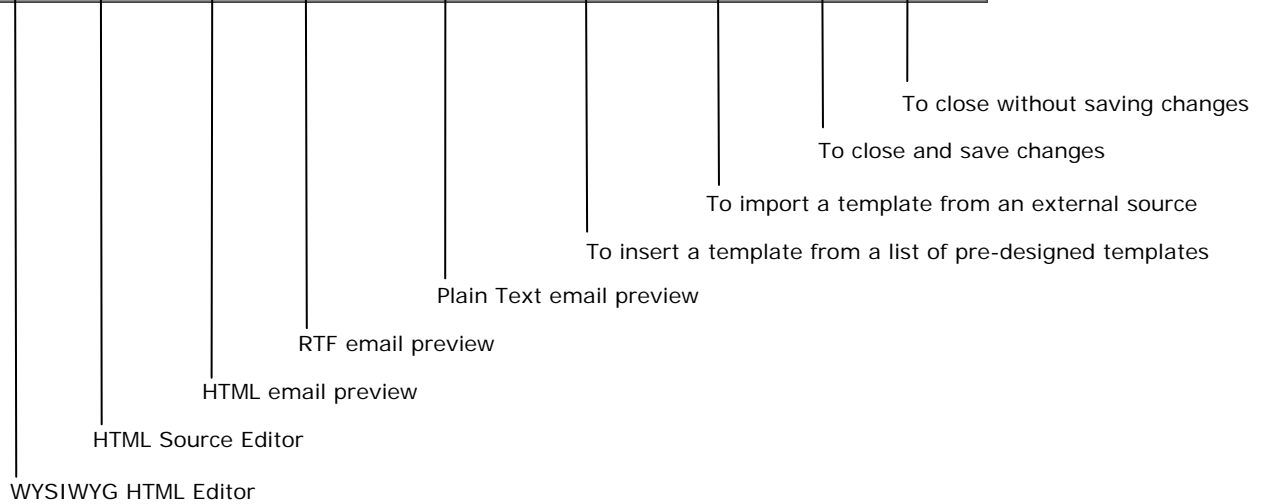
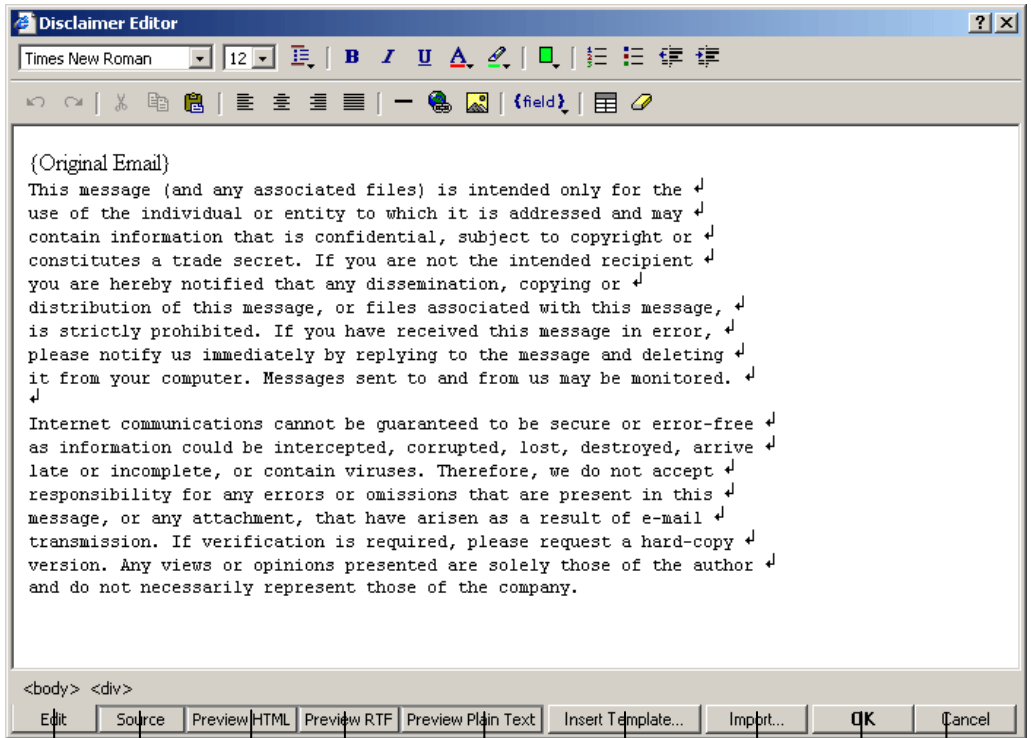
### The Disclaimer Editor box

Exclaimer Mail Utilities' Disclaimer Editor allows you to easily edit disclaimers, format the look of your email messages, add signatures, etc.

#### Button Descriptions



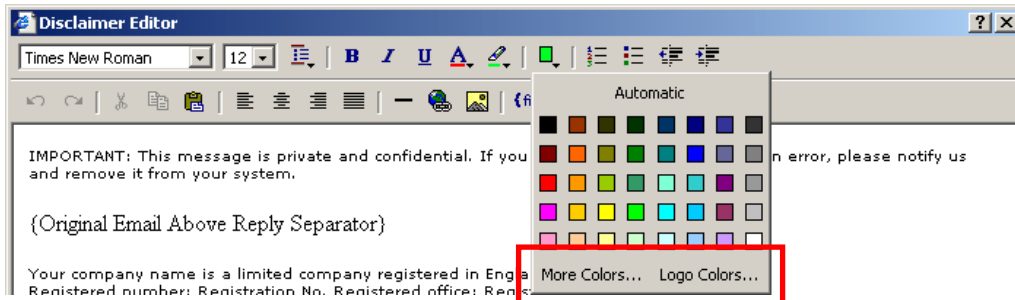




## Colors

This is where you select the colors you want to use for your text, text highlighting or background. You can access a more comprehensive list of colors by clicking on **More Colors** to open the **Colors** box.

Exclaimer Mail Utilities can also intelligently select the colors used in your organization's logo. You can view the logo colors tool by clicking on **Logo Colors**.

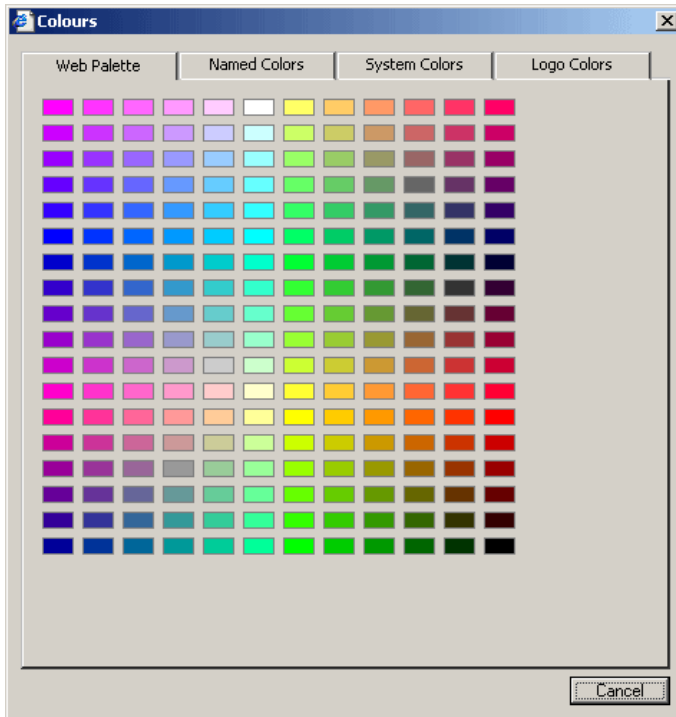


### The Colors box

The Colors box allows you to select from a wider range of colors. It contains four tabs that enable you to use a variety of different color types.

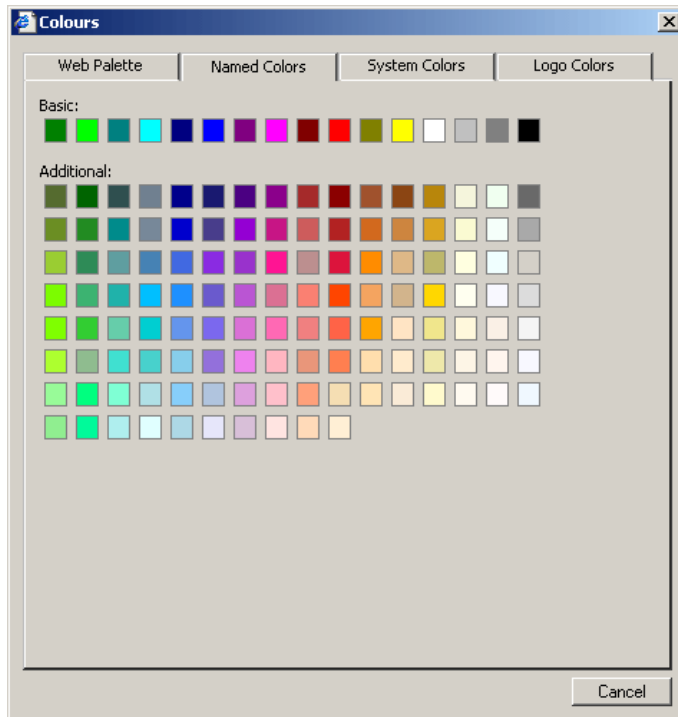
#### The Web Palette tab

This is where you can choose from the 216 standard web safe colors. Hover over the colors to find out their RGB color reference.



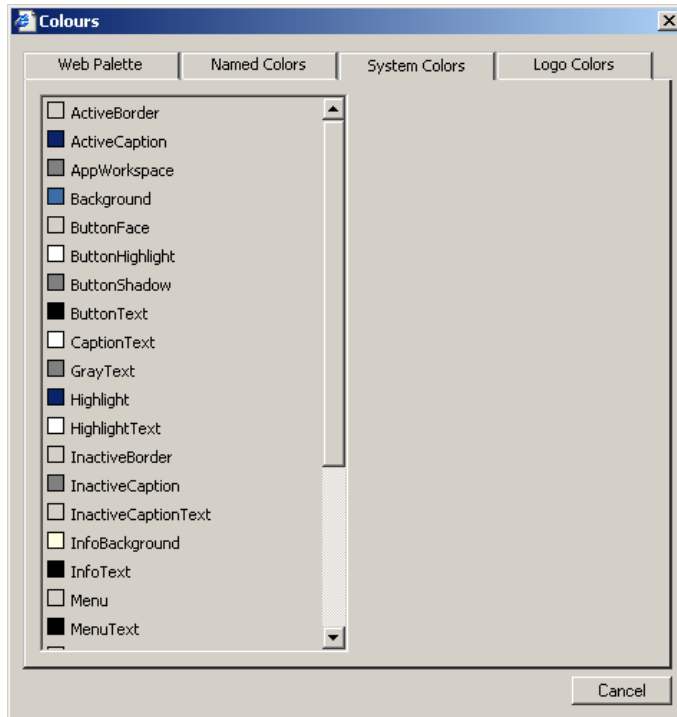
### The Named Colors tab

This contains a complete list of named web colors. Hover over the colors to find out their color reference.



### The System Colors tab

This contains a complete list of system colors that you can use in your email template. It will utilize the system colors used by the recipient's PC. The colors will change depending on the Windows color scheme they are using.



### The Logo Colors tab

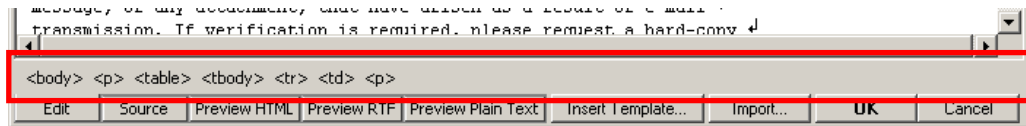
By default the Logo Colors feature automatically analyzes the logo in the Company logo User Defined Field and picks out the top fifteen most used colours. You can also select logos from other locations using the **Browse** button.

Hovering over the logo changes the mouse pointer into an eyedropper tool so you can pick individual colors from your logo. For more accurate selection of colors using the eyedropper tool you can zoom into the logo using the 200%, 400% and 800% radio buttons. As well as using the eyedropper tool you can also select from the top fifteen most used colors in the **Optimal colors from logo** palette. Hover over the boxes of color to find out their RGB color reference.



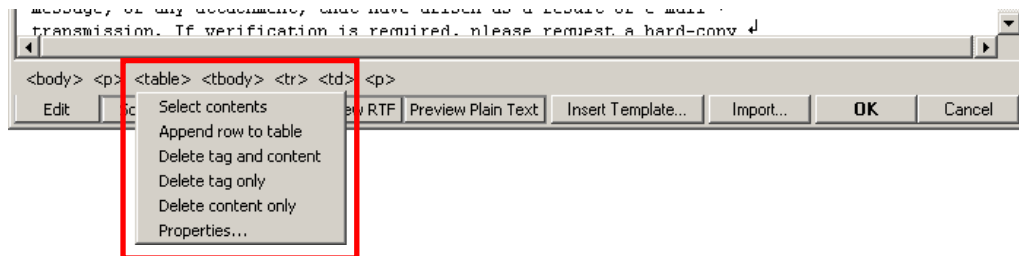
## HTML tag formatting toolbar

The HTML tag formatting toolbar appears near the bottom of the Disclaimer Editor window and displays the nested HTML tags leading to wherever the cursor is positioned on the page. Clicking on one of these tags displays a list of options:



## Tag Options

The tag options displayed here are for the **<table>** tag. Some tags will display more or fewer options.



The options that appear in the menu change depending on the tag you click on. They can include:

**Select contents** – selects the content of the tag.

**Delete tag only** – deletes the tag without deleting its content.

**Delete content only** – deletes the content of the tag only.

**Delete tag and content** – deletes both the tag and its content.

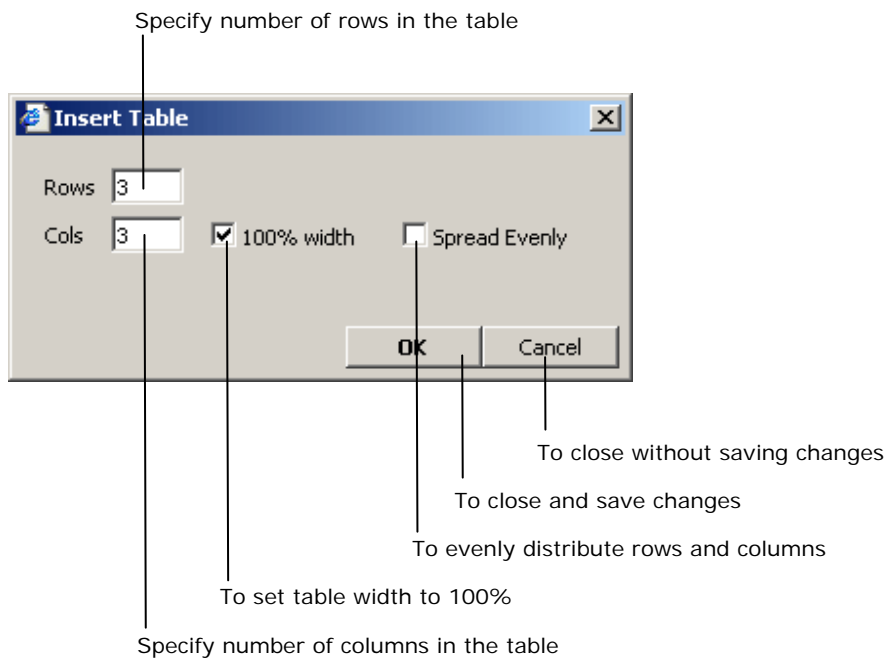
**Properties** – opens the **Properties box** where you can specify a tag's attributes. See **Properties box** on the next page for more information.

**Append row to table** – adds a row to the bottom of the table that your cursor is currently in.

**Append cell to row** – adds a cell to the end of the row that your cursor is currently in.

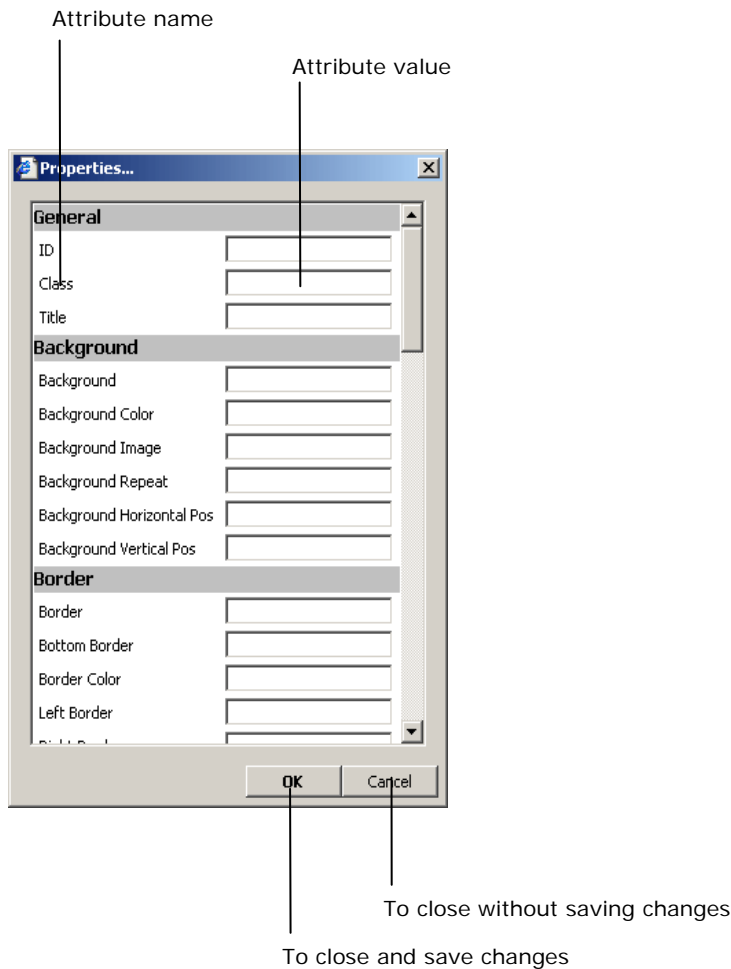
### Insert Table box

This is where you can specify the number of rows and columns in the table you are about to insert.



## Properties box

The Properties box is accessed through the Tag Options menu on the HTML tag formatting toolbar. This is where you can set the selected HTML tag's attributes.



## Avoiding blank AD fields appearing in email messages

To avoid empty AD fields appearing in your Exclaimer Mail Utilities formatted email disclaimer, signature, etc. You must add an Exclaimer IF statement to the HTML source code where the field appears. For example, you want to include a mobile telephone number field in your organization's email messages from your AD users. Some of your AD users don't have a work mobile telephone number but you don't want the field to appear blank in the email message.

### The solution:

```
<eXclaimer:if test="mobile">  
<DIV>Mobile: <eXclaimer:AD Field="mobile">{Mobile  
Number}</eXclaimer:AD></DIV></eXclaimer:if>
```

This IF statement will remove the text ('Mobile:') and field value from the email message if the AD field Mobile is blank. It is important to enclose the div tags that surround the text and AD field that you want to remove from the specified AD field is blank. This removes the field without leaving a blank line where it would have appeared.

### RTF and Plain text conversions

RTF and Plain text versions of email message branding, signatures and disclaimers are all converted from HTML into RTF and Plain text. When Exclaimer Mail Utilities converts messages from HTML into RTF it will remove table formatting and graphics from the template, leaving just the text and font formatting.

When it converts it to Plain text it will remove the remaining formatting leaving you with just the 'plain' text.

For example, you will find that messages sent in RTF will only contain text with no graphics or table layouts, limiting the corporate branding of your email to just text layout and font formatting.

#### **IMPORTANT!**

*Study the provided templates to understand the features available.*

*To save any changes you make in the Disclaimer Editor click on **OK**, then click on the **Save** icon in the left-hand menu.*

## ► Disclaimer Options

### The Disclaimer Options box

For configuring the way Exclaimer Mail Utilities sets the Character Encoding and Character Set. This is also where you select how you want Exclaimer Mail Utilities to disclaim different types of email message.

#### Option Descriptions

The screenshot shows the 'Disclaimer Options' dialog box with the following components and annotations:

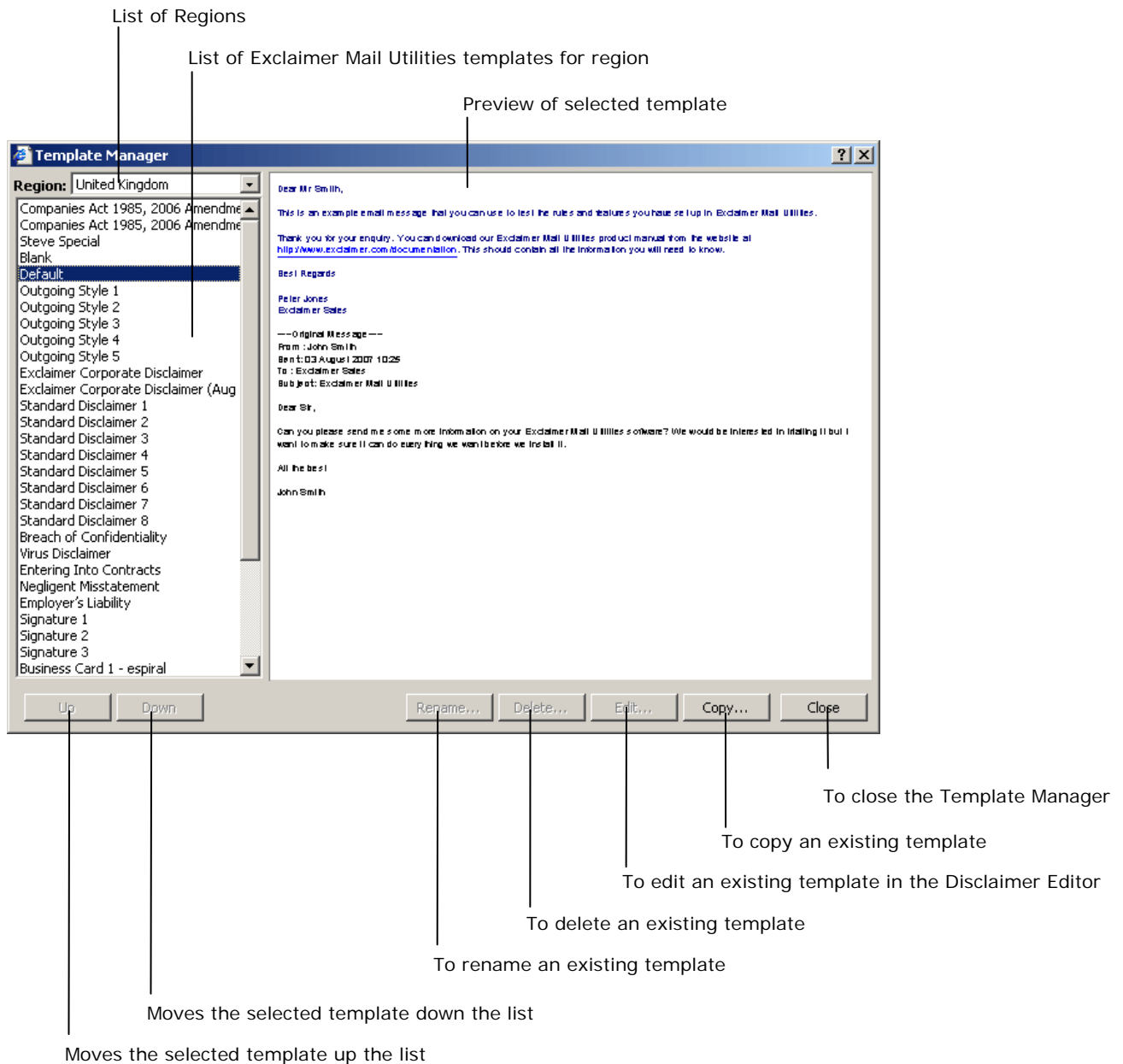
- HTML text encoding and character set:** Points to the HTML section, which includes 'Encoding method' and 'Character set' dropdown menus.
- Plain text encoding and character set:** Points to the Text section, which includes 'Encoding method' and 'Character set' dropdown menus.
- Message type:** A section with three options: 'Normal', 'Encrypted', and 'Digitally signed'. Each option has a dropdown menu for the message type, a text area for the disclaimer message, and a text field for the attachment name (all set to 'disclaimer.txt').
- OK button:** Labeled 'To close and save changes'.
- Cancel button:** Labeled 'To close without saving changes'.
- Annotations for message types:**
  - 'For selecting how you want Exclaimer Mail Utilities to deal with disclaimers on digitally signed messages' points to the 'Digitally signed' dropdown.
  - 'For selecting how you want Exclaimer Mail Utilities to deal with disclaimers on encrypted messages' points to the 'Encrypted' dropdown.
  - 'For selecting how you want Exclaimer Mail Utilities to deal with disclaimers on normal email messages' points to the 'Normal' dropdown.

## ▶ Templates

### The Template Manager box

For copying, creating new and editing Exclaimer Mail Utilities' pre-designed templates.

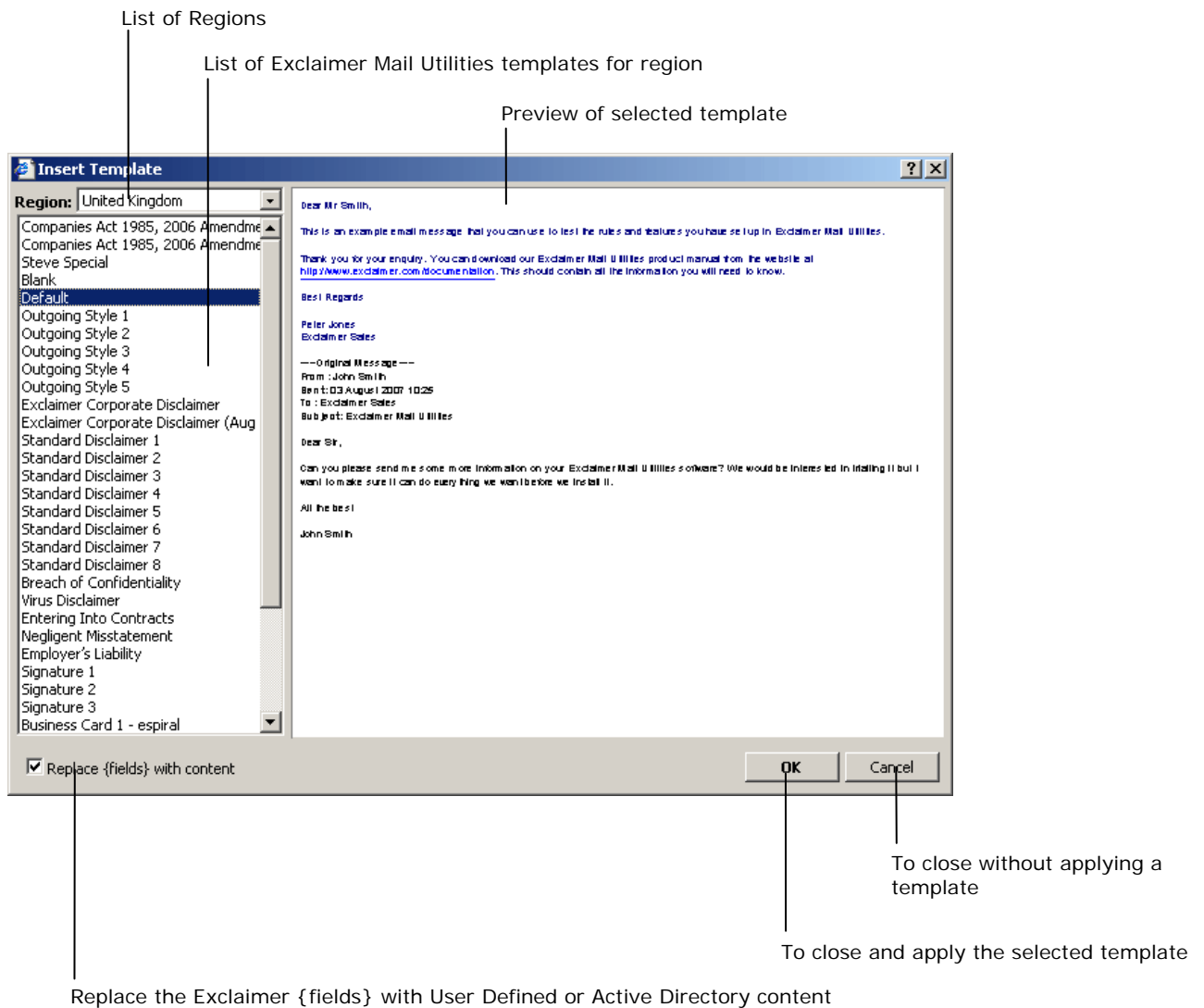
#### Button and Option Descriptions



## The Insert Template box

Where you select the template that you want to use. If you want to create a new template go to **Setup** on the Exclaimer Mail Utilities' Control Panel, click on **Templates...** and copy the template that you want to use as the basis of your new template. See *The Template Manager Box* section on the previous page.

### Button Descriptions



**IMPORTANT!**

*A template is essentially a re-usable disclaimer and may contain text formatting, graphic images and fields.*

*You create and modify templates using the Disclaimer Editor, see the Disclaimer Editor section.*

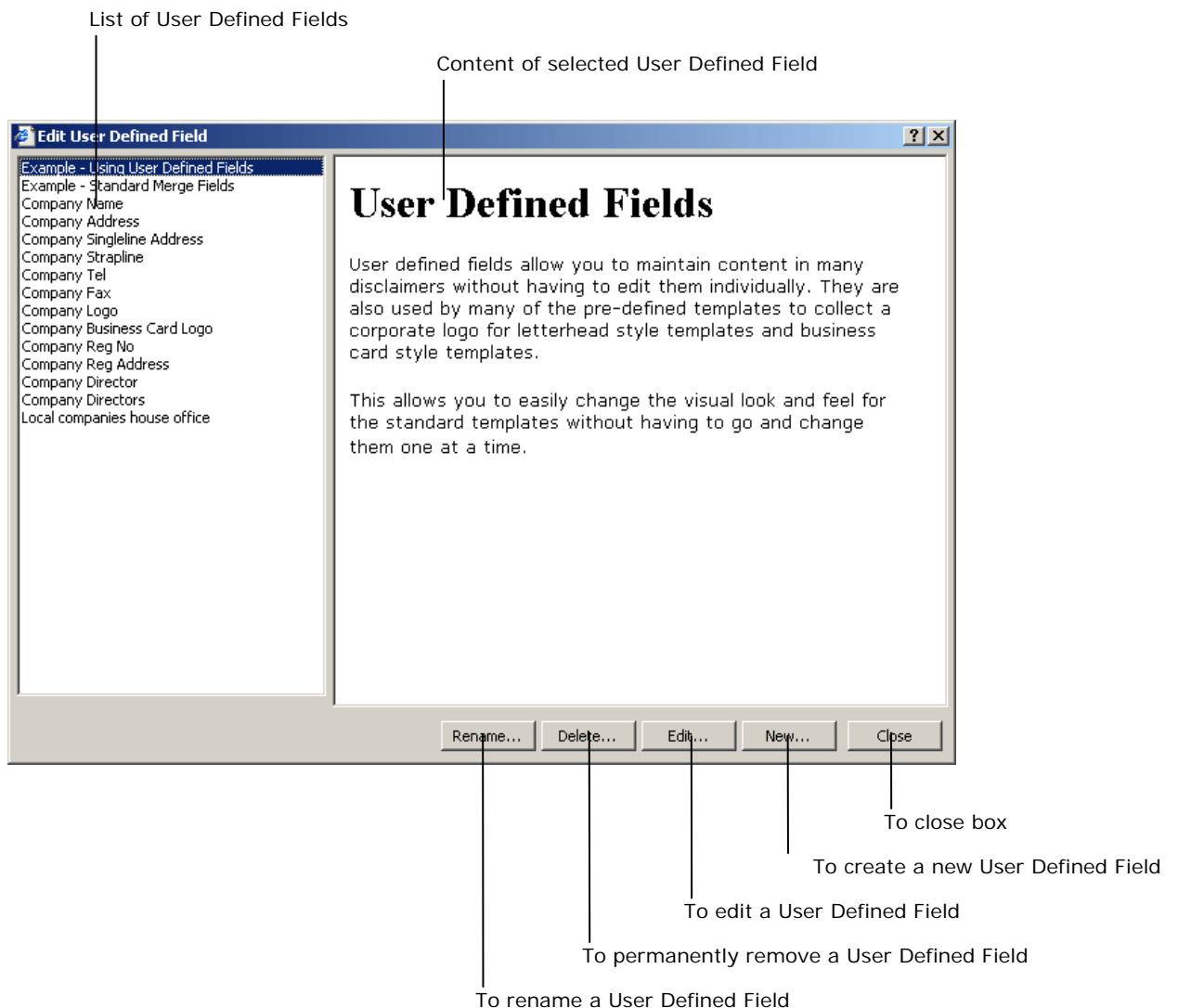
*If you choose a template that includes User Defined Fields you may be asked to provide information for use in these fields.*

## ▶ User Defined Fields

### The User Defined Fields box

Exclaimer Mail Utilities' User Defined Fields allow you to set specific types of company information that is relevant to all users. You can even create you own User Defined Fields to contain any information you like. These fields can then be used in Exclaimer Mail Utilities' pre-designed email templates and disclaimers.

#### Button Descriptions



Note – you can also find a list of the standard Exclaimer Mail Utilities' merge fields by clicking on **Example –**

**Standard Merge Fields** in the list of User Defined Fields, which can be to the left of the Edit User Defined Fields box.

#### **Creating a new User Defined Field**

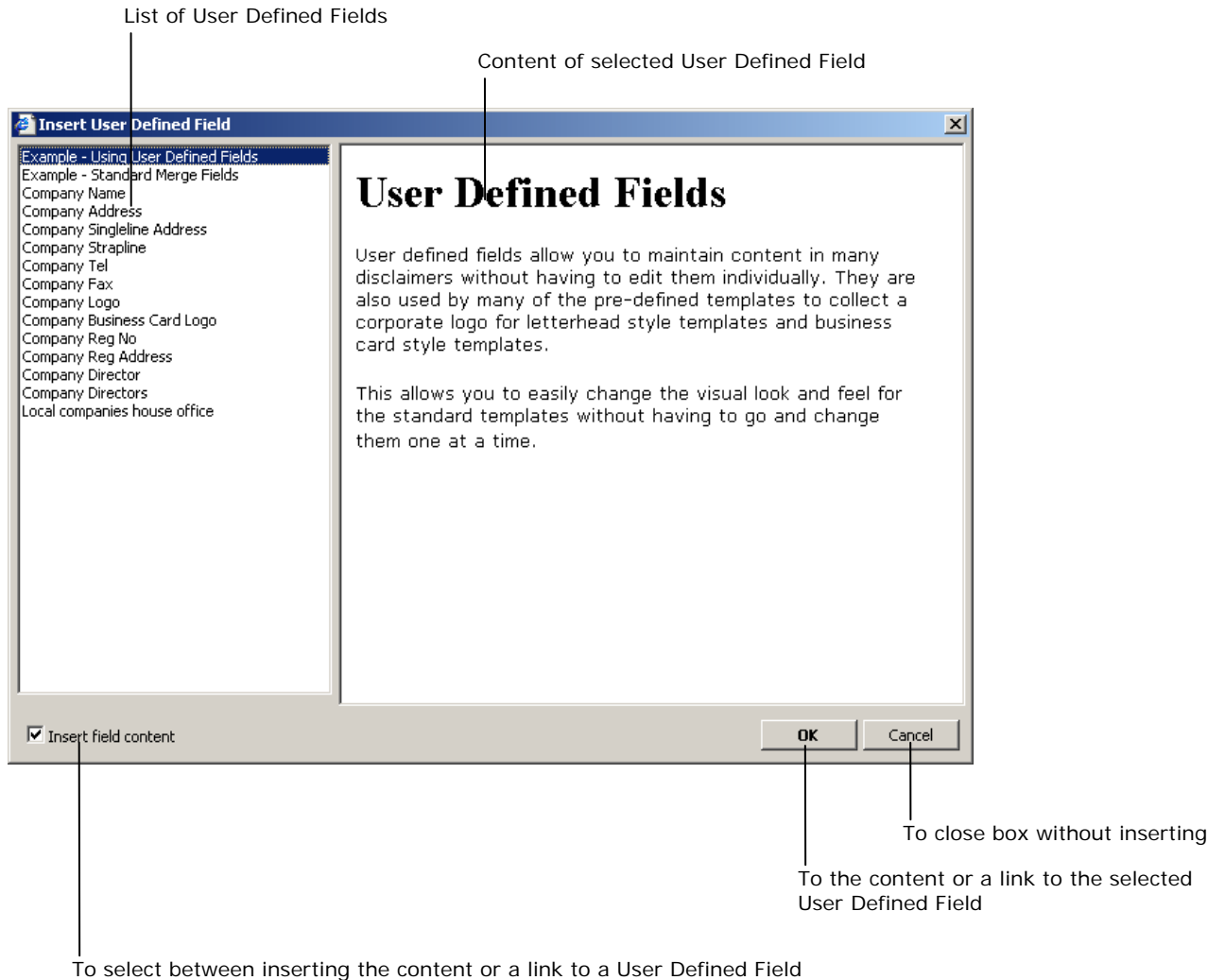
Clicking on **New** will open the **Disclaimer Editor** where you can format the selected User Defined Field using the tools available, changing the look of the text or other contents of the field.

You are limited to editing the contents of the Company User Defined Fields in a simple text box only. You cannot use any type of formatting on the text into these fields. If you require a User Defined Field with formatted text you can do so by creating a new one and editing it in the Disclaimer Editor.

## The Insert User Defined Fields box

This is where you can insert either the contents (which can include html mark-up, images and other formatting) or a link to a User Defined Field allowing you to update content outside of the email/disclaimer template you are currently editing.

### Button Descriptions



## ▶ Active Directory Attribute Query Editor

### The Active Directory Attribute Query Editor box

Exclaimer Mail Utilities' Active Directory Attribute Query Editor allows you to easily create rules based upon combinations of attributes in your Active Directory.

#### Field and button descriptions

The name of the rule

The Active Directory container

To browse the AD containers

To use the domain controller

The screenshot shows the 'Active Directory Attribute Query Editor' dialog box. It features a title bar with a question mark and close button. Below the title bar is a text area with a brief description of the tool's purpose. The main interface is divided into several sections: 'Rule name' (a text input field), 'Container' (a text input field with a 'Browse...' button and a 'Use domain controller' checkbox), 'Query Wizard' (a section with a 'Start with' dropdown set to 'No one' and a rule builder area containing a 'then' clause with 'Add' and 'users where' options, and several dropdown menus for attribute selection), 'Analysis' (an empty text area), 'Test columns' (an empty text area), and 'Test Results' (an empty text area). At the bottom, there is a 'Test only returns top' field set to '100' rows, and buttons for 'Advanced', 'Test...', 'OK', and 'Cancel'.

To add a query string

To remove a query string

To start the query with all AD users or no users

To add or remove users that match the following query

Select the field you want to query

Select how you want to query it

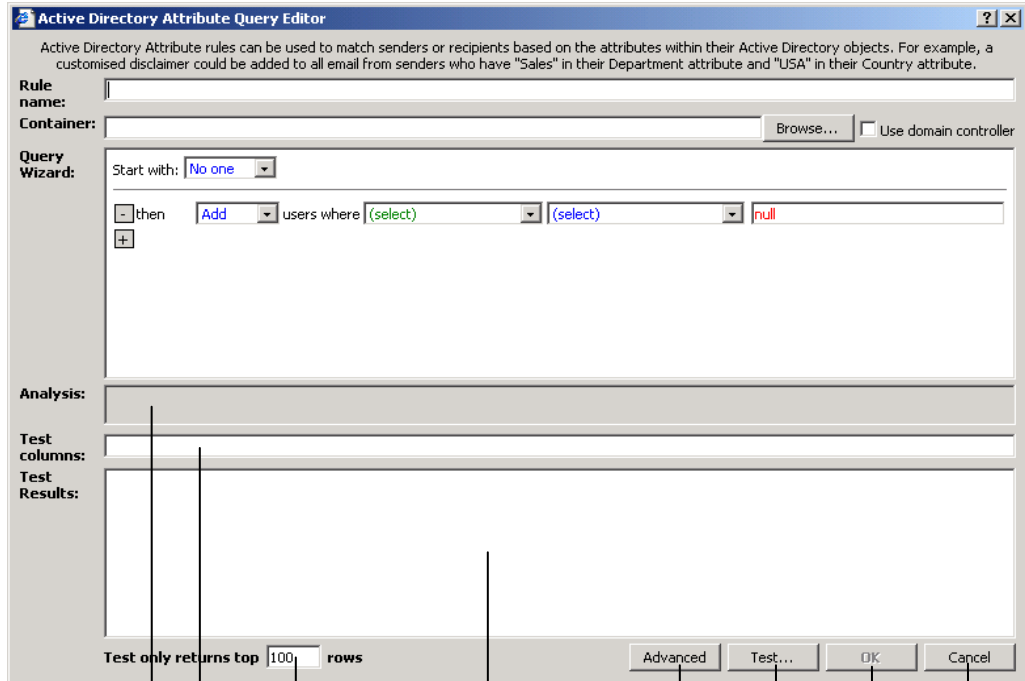
Type the value you are looking to match

The screenshot shows the 'Active Directory Attribute Query Editor' window. The title bar reads 'Active Directory Attribute Query Editor'. Below the title bar is a help text: 'Active Directory Attribute rules can be used to match senders or recipients based on the attributes within their Active Directory objects. For example, a customised disclaimer could be added to all email from senders who have "Sales" in their Department attribute and "USA" in their Country attribute.'

The window contains several sections:

- Rule name:** A text input field.
- Container:** A text input field with a 'Browse...' button and a checkbox for 'Use domain controller'.
- Query Wizard:** A section for building the query. It starts with 'Start with: No one' (dropdown). Below this is a sequence of actions: a minus sign button, 'then', 'Add' (dropdown), 'users where', '(select)' (dropdown), '(select)' (dropdown), and 'null' (dropdown). A plus sign button is at the bottom left of this section.
- Analysis:** A large empty text area.
- Test columns:** A large empty text area.
- Test Results:** A large empty text area.

At the bottom of the window, there is a status bar that says 'Test only returns top 100 rows' and buttons for 'Advanced', 'Test...', 'OK', and 'Cancel'.



- Indicates whether the analysis was successful
- Displays columns that are queried
- To limit the number of rows the test returns
- Displays the test results
- To switch between Advanced and Basic query mode
- To test the query
- To close and save the query string
- To close without saving

**Rule name:** - This is where you enter the name of your custom rule. It is best to name the rule with a description that helps to identify what the rule does. You may also find it useful to enter when changes were made to a rule, if you have many people administering your server.

**Container:** - You can choose to select a specific Active Directory Container for the query search. If you leave this field blank Exclaimer Mail Utilities will search the entire Active Directory.

Click on the **Browse...** button to select the Active Directory Container you want to use.

**Use domain controller** – Place a tick in the **Use domain controller** checkbox if you want your query to only use attributes that are held by the Domain Controllers. Please note that your query will fail for users in other domains.

**Query Wizard:** - Enter the query strings you want to use to trigger your custom rule.

**Analysis:** - Displays the status of the query test.

**Test columns:** - Lists the columns used to perform the query.

**Test Results:** - Displays the results of the query strings in the Query Wizard section.

**Test only returns top** – Enter the maximum number of rows you want to appear in the Test Results section.

**Advanced** – Select between the advanced and basic query mode. The Advanced mode allows you to type in the query strings manually.

**Text...** - When you test your query you may be warned that some of the attributes you used are not indexed. This will result in a slow query. Consider creating a different query, or editing your Active Directory schema to index the attribute.

**IMPORTANT!**

To save any changes you make in the Active Directory Attribute Query Editor click on **OK**, then click on the **Save** icon in the left-hand menu.

**Attribute Query Example:**

If your organization has offices throughout the world, you can create a set of rules that apply a different disclaimer depending on the value set in the **Country (C)** Active Directory Attribute field. This would allow you to create a set of disclaimers that you can deploy from a central location to comply with local regulation. For example, you could create a rule that adds a country specific disclaimer to email messages sent from users in Great Britain (GB).

The screenshot shows the 'Query Wizard' interface. It features a 'Start with:' dropdown menu set to 'No one'. Below this, there is a rule configuration area with a minus sign button, a 'then' label, an 'Add' dropdown menu, the text 'users where', a 'Country' dropdown menu, the text 'is equal to', another dropdown menu, and the value 'GB'. A plus sign button is located at the bottom left of the rule configuration area.

# Index

## About Panel

- Licensed Customer Details, 93
- Licensed Product Details, 93
- Support Details, 93
- Version Information, 93

## About Panel, The, 93

## Active Directory Attribute Query Editor, Exclaimer's, 115

## Add Mail Rule box

- Addressing tab, 55
  - Active Directory Attributes, 56
  - Active Directory Container (Organizational Unit), 56
  - Active Directory Users and Groups, 56
  - Any Active Directory Contact, 56
  - Anyone, 55
  - Anyone External, 56
  - Anyone in the Active Directory, 56
  - Anyone Internal, 55
  - Anyone with an X400 address, 56
  - Email Address, 56
  - Email Domain, 56
  - Message header equals, 57
  - Rule name, 57
  - Sender/Recipients, 55
  - Subject contains, 57
- Auto-responder tab
  - Auto-responder, 61
  - Options sub-tab, 64
    - Loop detection, 64
    - Message format, 64
  - Sender + Recipients sub-tab, 63
    - Auto-response reply-to address, 63
    - Auto-response should appear to be from, 63
    - BCC Auto-response to, 63
    - CC Auto-response to, 63
    - Send auto-response to, 63
    - Send auto-response to original sender, 63
  - Subject + Content sub-tab, 62
    - Append text to subject, 62
    - Attachments, 62
    - Auto-response message, 63
    - Edit/Preview response..., 63
    - Message Body, 62
    - Prepend text to subject, 62
    - Reply using original subject, 62
    - Reply using this subject, 62
    - Response options, 63
    - Subject, 62
  - then process next applicable auto-responder rule, 62
- Auto-responder tab, 61
- Delivery Options tab, 58
  - Convert MIME message to plain text, 59
  - Deliver the message but change the destination as follows, 58
  - Deliver the message but change the From and Reply To addresses, 58
  - Deliver the message to the original recipients, 58
  - Delivery Options, 58
  - Do not deliver the message to anyone, 58
- Disclaimers tab, 59
  - Disclaimer, 59

## Disclaimer options..., 60

- Don't add disclaimer if Body contains, 59
- Don't add disclaimer if subject contains, 60
- Edit/Preview disclaimer..., 60
- then process the next applicable disclaimer rule, 59

## Message Journaling tab

- Journal copies to, 61
- Journal external mail, 61
- Journal internal mail, 61
- then process next applicable external journaling rule, 61
- then process next applicable internal journaling rule, 61

## Message Journaling tab, 60

## Rule enabled, 58

## Add Mail Rule box, The, 55

## Advanced Settings box

- Active Directory tab, 44
    - Cache the Active Directory search objects, 44
    - Credentials, 45
    - Domain Controller, 44
    - Global Catalog, 44
    - TLL, 44
  - Anti-Spam tab, 47
    - Bounce Message, 48
    - SPF Best Guess Policy, 47
  - Categorizer tab, 41
    - Bifurcate non-TNEF messages that are categorized as both internal and external, 42
    - External Domains, 41
    - Internal Addresses, 41
    - Internal Domains, 41
    - Treat all contacts as external addresses, 42
  - Defer anti-spam checks until after DATA command, 48
  - DNS tab, 42
    - DNS Servers, 42
    - Relay Servers, 42
  - Error Handling tab, 46
    - Deliver message anyway, 46
    - Discard the message, 46
    - Error Handling, 46
    - Folder, 47
    - Notify Sender of the Error Handling Action, 47
    - Quarantine the message but if that fails deliver the message anyway, 47
    - Quarantine the message but if that fails stop the SMTP service, 47
    - Quarantine will fail if there are more than # messages already quarantined, 47
  - Identifiers tab, 38
    - Message Classes, 40
    - Reply Separator, 38
  - Performance tab, 46
  - Proxy Server tab, 43
    - Proxy Authentication, 43
    - Proxy Server Address, 43
    - Proxy Server Port, 43
    - Use Proxy Server, 43
    - User name/Password, 43
- ## Advanced Settings box, The, 38
- ## Anti-Spam Settings Panel
- Advanced tab, 72

- Action, 72
- Include Critical, 72
- Result, 72
- Rule, 72
- Then, 72
- Options tab, 68
  - Anti-Spam quarantine mailbox, 68
  - Backdoor/Challenge code, 68
  - Manual Blacklist, 68
  - Manual Whitelist, 68
  - Mission Critical Accounts, 68
- Scenarios tab, 70
  - Custom, 71
  - Deployed (Recommended), 70
  - End user rollout, 70
  - Evaluation, 70
  - Hardened, 71
  - Quarantined, 70
- Spam tests
  - Auto Whitelist, 76
  - Blocked IP, 73
  - Detection Center, 77
  - Detection Center - Bulk, 78
  - Detection Center - Bulk (SPF\_PASS), 78
  - Detection Center - Spam, 78
  - DNS Blacklist, 77
  - DNS RHS Blacklist, 77
  - DNS RHS Whitelist, 77
  - DNS Whitelist, 76
  - Email with attachment, 79
  - HTML Emails, 78
  - Manual Whitelist, 75
  - Mission Critical Accounts, 73
  - Mission Critical Manual Blacklist, 73
  - Recipient not in the AD, 74
  - SPF Fail, 75
  - SPF PASS, 78
  - SPF Softfail, 76
  - Spoofed Domain, 74
  - Spoofed IP, 74
  - Trusted IP, 75
  - Unclassified, 79
- Anti-Spam Settings Panel, The, 68
- Anti-Virus Settings Panel
  - Action, 80
  - Result, 80
  - Rule, 80
  - Then, 80
  - Virus tests
    - Detection Center - Maybe virus, 81
    - Detection Center - Virus, 81
- Anti-Virus Settings Panel, The, 80
- Applying a license, 94
- Custom Rules Panel
  - Add rule..., 53
  - Copy..., 53
  - Delete, 53
  - Edit..., 53
  - Recipient ↓ (Decrease), 54
  - Recipient ↑ (Increase), 53
  - Sender ↓ (Decrease), 53
  - Sender ↑ (Increase), 53
  - Validate..., 54
- Custom Rules Panel, The, 53
- Default Rules Panel
  - Disclaimer tab, 49
    - Disclaimer options, 50
    - Don't add disclaimer if body contains, 50
    - Don't add disclaimer if subject contains, 50
    - Edit/Preview disclaimer..., 50
    - Incoming, 49
    - Internal, 49
    - Outgoing, 49
    - Remove from subject, 50
  - Message Journaling tab, 52
    - Journal copies to, 52
    - Journal incoming mail, 52
    - Journal internal mail, 52
    - Journal outgoing mail, 52
- Default Rules Panel, The, 49
- Disclaimer Editor, 96
  - Colors, 99
  - HTML tag formatting toolbar, 104
  - Insert Table box, 105
  - Logo Colors tab, 103
  - Named Colors tab, 101
  - Properties box, 106
  - System Colors tab, 102
  - Web Palette tab, 100
- Disclaimers. *See* Default Rules Panel, The or Custom Rules Panel, The
- Insert Template box, The, 110
- Insert User Defined Fields, The, 114
- Logging and Statistics Panel
  - Logging tab, 82
    - Enabled, 82
    - Errors, 82
    - Folder, 82
    - Keep file for, 82
    - Log files, 83
    - Message flow, 82
    - Transactions, 82
    - Warnings, 82
  - Statistics tab
    - Copy, 92
    - Exclaimer DLL, 91
    - Exclaimer Emails Processed, 83
    - Exclaimer Errors & Warnings, 86
    - Exclaimer Features, 84
    - Exclaimer Spam Engine Counters, 86
    - Exclaimer Throughput, 90
    - Exclaimer Timings, 88
    - Exclaimer Virus Engine Counters, 88
    - Refresh Stats, 92
    - Reset Stats, 92
  - Statistics tab, 83
- Logging and Statistics Panel, The, 82
- Main Menu
  - About. *See* About Panel, The
  - Anti-spam. *See* Anti-Spam Settings Panel, The
  - Anti-virus. *See* Anti-Virus Settings Panel, The
  - Custom Rules. *See* Custom Rules Panel
  - Default Rules. *See* Default Rules Panel, The
  - Logging & Stats. *See* Logging and Stats Panel, The
  - Rule Tester. *See* Rule Tester Panel, The
  - Save, 28
  - Setup. *See* Setup Panel, The
- Main Menu, The, 27
- Passwords, 37
- Remote Deployment box, The, 33
- Rule Tester Panel
  - Attachment, 65
  - Basic/Advanced test results box, 67
  - Message Section, 66
  - Preview window, The
    - Auto-response, 66
    - Final Message, 66
    - Journal Message, 66
    - Original Message, 66
  - Preview window, The, 67
  - Recipient, 65
  - Run advanced test, 66
  - Run basic test, 66
  - Sender, 65
  - Subject, 65

**Rule Tester Panel, The, 65**  
**Set Passwords box, The, 37**

**Setup Panel**

Admin Contact, 29  
Anti-Spam, 32  
Auto Responding, 32  
Enable Disclaimers, 30  
Enable Envelope Journaling, 32  
Enable Exclaimer, 29

Error Handling Messages, 30

Message Journaling, 30

Rule Conflict Reports, 29

Suppress read receipts from all journal accounts,  
30

Zero-Hour™ Virus Protection, 32

**Setup Panel, The, 29**

**Template Manager box, The, 108, 109**

**User Defined Fields, The, 112**