Exclaimer Auto Responder
User Manual

Exclaimer
UK +44 (0) 1252 531 422
USA 1-888-450-9631
info@exclaimer.com

Contents

Introduction 9
How does it Work? 9
But That's Not All... 10
And There's More... 10
Installation 11
Introduction 12
The Installation Wizard 13
The Configuration Wizard 14
Setting Up Multiple Servers 14
The Exclaimer Console 15
Introduction 16
Understanding the Exclaimer Console Window 17
Exclaimer Console Summary 17
Exclaimer Console Settings 23
Actions 25
Exclaimer Console Licensing 27
The Licensing Process 28
Licensing Information 28
The Licensing Toolbar 28
Actions 29
Exclaimer Console Status 30
Filtering the Status List 31
The Status Toolbar 32
Actions 32
Remote Deployment 34
How it Works 35
The Remote Deployment Folder 35
Remote Deployment Timings 36
Changing an Existing Remote Deployment Folder 37
Saving Changes in the Exclaimer Console 38
Exporting Configuration Settings 39
Importing Configuration Settings 39

General Settings & Information for Auto Responder 40
Introduction 41
Auto Responder Settings 43
Available Settings 44
Advanced Settings 45
The Settings Toolbar 47
Actions 47
Auto Responder Policies 49
The Policy List 50
The Policies Toolbar 50
View Options 51
Actions 52
Auto Responder Status 53
Filtering the Status List 54
Filter by Time Period 54
Filter by Status Type 54
Filter by Time Period and Status Type 54
The Status Toolbar 54
Status Information Retention 55
Actions 55
Working with Auto Responder Policies 57
Introduction 58
Action(s) to be Taken 58
Circumstances under which a Policy is Triggered 58
Content Required for an Action 58
Policy Types 60
Automatic Reply 60
Message Redirection 61
Sender Modification 61
Add Recipients 62
Ethical Walls 62
Advanced 63
Accessing Existing Policies 64
Navigating Policies Using the Console Tree 64
Navigating Policies Using Policy Tabs 66

The Policies List 67
The Policy List 68
The Policy Setup Pane 69
The Policies Toolbar 69
View Options 70
Actions 70
The Anatomy of a Policy 72
The Anatomy of a Policy - General 73
The Anatomy of a Policy - Original Message 74
The Anatomy of a Policy - Auto Response 78
The Anatomy of a Policy - Template 83
The Template Breadcrumb Trail 83
The Anatomy of a Policy - Conditions 84
Available Options for Setting Conditions 85
Creating Queries With the Configure Attributes Window 89
The Anatomy of a Policy - Exceptions 91
Available Options for Setting Exceptions 92
The Anatomy of a Policy - Date Range 96
Using the Advanced Schedule 97
The Anatomy of a Policy - Next Policy 98
Adding Auto Responder Policies 99
Adding an Automatic Reply Policy 100
Adding a Message Redirection Policy 108
Adding a Sender Modification Policy 112
Adding an Add Recipients Policy 116
Adding an Ethical Walls Policy 119
Adding an Advanced Policy 125
Cloning a Policy 128
Changing a Policy 129
Enabling and Disabling a Policy 129
Removing a Policy 130
How To 131
How do I Change the Template Associated with a Policy? 132
Steps 1 - 3: Access the Template Library from Within a Policy 132
Steps 4 - 6: Browse and Select New Templates 133
How do I Change the Sequence in which Polices Run? 134
How do I Create a Policy Based upon Specific Active Directory Attributes? ... 135

Steps 1 and 2: 'The Sender is Someone' 135
Steps 3 and 4: 'The Sender has One or More Specific AD Attributes'..... 136
Steps 5 and 6: Enter Basic Details for the Query 137
Steps 7 and 8: Browse and Select an Active Directory Container..... 138
Steps 9 and 10: Choose a Start Point and Select Required Attribute 139
Step 11: Choose how Matching Should be Made 140
Step 12: Enter the Required Attribute Value for Matching 141
How do I Block Emails between Two Parties? 142
How do I Define a Policy Based upon a Subject Line Trigger Word? 144
Step 1: Select 'The Subject Contains Specific Words or Phrases' Option ... 144
Step 2: Add Required Words and Phrases 145
Step 3: Set Options for Words and Phrases..... 146
How do I Create a Policy for All Internal or All External Emails? 147
Step 1: Access Policy Conditions and Select 'The Recipient Is Someone'... 147
Step 2: Click the 'Someone' Link in the Lower Pane 148
Step 3: Select 'Recipient is Inside or Outside of the Organization' 148
How can I Send File Attachments with an Automatic Reply? 149
How do I Implement an Out of Office Reply?..... 150
The Policy Tester.....151
Introduction 152
Understanding the Policy Tester Window 153
The Policy Tester Toolbar 154
The Email Editor Toolbar 154
Additional Options..... 154
Security Settings 154
Message Settings..... 154
Delivery Options 155
Headers..... 155
Creating a New Policy Test 156
Saving and Re-Using a Policy Test 157
Saving a Policy Test 157
Re-using a Saved Policy Test 157
Working with Rules Applied Information 158
Checking the Reason Why A Policy Is or Is Not Applied..... 160
Previewing the Message at any Stage in the Process 161
Working with Test Messages..... 162

The Template Library 163
Introduction 164
Understanding the Template Library Window 165
The Console Tree 166
The Template Library Toolbar 166
The Template Library Content Pane 167
View Options 167
Actions 167
Working with Categories 169
Adding a New Category 170
Renaming a Category 171
Removing a Category 172
Working with Templates 173
Previewing a Template 174
Adding a New Template 175
Cloning a Template 177
Exporting a Template 178
Importing a Template 178
Editing a Template 179
Renaming a Template 180
Moving a Template 181
Viewing Template Properties 182
Removing a Template 183
The Template Editor 184
Understanding the Template Editor Window 185
Using Fields in Templates 198
Working With the Fields Panel 199
Techniques for Working with Fields 200
Using Spaces Between Fields 200
Copying and Pasting Original Message Fields 200
Available Fields 201
Message Fields 201
Message Sender Fields 202
Message Recipient Fields 209
Dynamic Content Fields 215
Server Fields 224
General Fields 224

Properties 225
Working With the Properties Pane 226
How To 229
How can I Tell which Policies are Using a Specific Template? 230
How do I Include the Original Message in an Automatic Reply? 231
How do I Set the Font for Text in an Automatic Reply? 232
How do I Suppress Blank Lines if Fields are not Populated? 233
Use a Contact Block 233
Use a Field Prefix 234
How do I Create a Contact Block? 235
Example of a contact block 235
How it works 235
Updating an Existing Contact Block 237
How do I Insert a Banner Image at the Start of Messages? 239
Other Resources 240
Exclaimer Support 240
Exclaimer Sales 240
Copyright Notice 241

Introduction

Exclaimer Auto Responder provides full, centralized control over automated response actions to be taken with email. Auto Responder can help you to maintain a professional, consistent approach when sending automated replies to email messages, and can help to manage the flow of email under a given set of circumstances.

Traditionally, an automated response is thought of in terms of a predefined email response that is sent automatically upon receipt of an incoming message - one of the most common examples being an Out of Office reply.

Within Auto Responder this kind of automated response can certainly be defined, however the concept of an automated response goes much further. Exclaimer Auto Responder considers an automated response to be an action that is taken upon the transmission of an email message; in some situations that action will be the transmission of an automatic reply [see page 60], but in other situations it could be any of the following scenarios:

- Message redirection [see page 61] - where incoming email messages are redirected to an alternative mailbox.
- Sender modification [see page 61] - where sender information is changed before email messages are transmitted.
- Add recipients [see page 62] - where one or more recipients are added before email messages are transmitted.
- Ethical walls [see page 62] - where email transmission is blocked between specified parties.

How does it Work?

Within Exclaimer Auto Responder, you control automated responses by defining a number of elements, as summarized below:

- The **type** of automated response required (select a policy type [see page 60] based upon predefined scenarios listed above, or create your own using the advanced policy type [see page 63])
- The **circumstances under which the automated response should be triggered** (using conditions [see page 84], exceptions [see page 91], date range [see page 96] and next policy [see page 98] options)
- **What happens to the original email message** before / after transmission (using original message [see page 74] options)
- The **content and behavior of an automated reply message**, if applicable (using templates [see page 164] and auto response [see page 78] options respectively)

These elements are defined and combined using policies. You can create as many policies as required - for example, you might choose to send different automated replies for each department within your organization and so create one automatic reply [see page 100] policy for each department. Or, you might choose to send different automated replies on weekdays and weekends [see page 96], or based upon the subject line of incoming emails [see page 84], etc.

Similarly, you might need to define a number of policies of different types. For example, you might use automatic reply [see page 100] policies in addition to message redirection [see page 108] policies and a range of ethical walls [see page 119] policies. The possibilities are immense and can all be achieved using Exclaimer Auto Responder.

But That's Not All...

Exclaimer Auto Responder includes a library of professional templates [see page 164] which can be used as the basis of an automatic reply. You can edit these templates, or create new ones (including tables, images and dynamic Active Directory fields) using an intuitive template editor [see page 184]. Templates can be created in either HTML or Plain Text formats, with an instant preview [see page 174] feature so you can see, at a glance, how your template will be displayed in email messages.

And There's More...

Perhaps one policy isn't enough; perhaps you need to perform (or not perform) certain automated responses based upon whether or not a previous policy was applied. With Exclaimer Auto Responder, you can create policy chains [see page 98] to define such dependencies.

And there's no need to worry about complicated testing processes, since an intuitive policy tester [see page 152] is included which will simulate the process of sending and receiving emails so you can quickly see if policies have been defined correctly.

Chapter 1

Installation

Introduction

The Exclaimer Auto Responder installation process is comprised of two parts - installation [see page 13] and configuration [see page 14]. Both stages are quick and easy to complete, using a familiar 'wizard' approach to guide you through each process, step-by-step.

The installation process includes the Exclaimer license agreement and copies files to your preferred destination folder. Once complete, the configuration wizard is launched, so you can configure basic settings for Exclaimer Auto Responder, which will enable you to get started as soon as the wizard is complete.

The Installation Wizard

To install Exclaimer Auto Responder, follow the steps below:

1. Double click the setup file to start the process and display a welcome message.
2. Click setup to launch the setup wizard.
3. Click next to view the end-user license agreement.
4. Having read the license agreement, check the I accept the terms in the license agreement box.
5. Click next to select a destination folder for installed files. From here you can accept the default folder, or click change to specify a new location.
6. Click next to confirm the destination folder and prepare the installation.
7. Click install to perform the installation.
8. Once files are copied, click finish. The installation is now complete and the configuration wizard [see page 14] is launched so you can confirm basic settings and get started with Exclaimer Auto Responder.

The Configuration Wizard

Having run an installation [see page 13] for Exclaimer Auto Responder, the configuration wizard is launched so you can complete basic setup options and get started straight away. To complete this wizard, follow the steps below:

1. The first stage of the configuration wizard displays summary information about the process.
2. Click next to move to the next stage and set an administration mailbox. If required, click the browse button to browse user accounts and make a selection. The account specified will receive notification emails from Exclaimer Auto Responder.
3. Click next to move to the next stage and view summary information.
4. Click finish to complete the process and start the new policy wizard [see page 99]. This wizard guides you through the process of creating your first Auto Responder policy, so you can quickly get started with the application.

> If you wish to manage multiple servers, you should also check remote deployment options (see *Setting Up Multiple Servers*, below).

Setting Up Multiple Servers

Exclaimer Auto Responder can be run on multiple servers and managed from a single location. This means that (even on very large systems) you can ensure all of your email systems have the same policies, templates and settings installed so email is processed consistently across the entire organization.

To achieve this, the installation [see page 13] and configuration [see page 14] must be run on each, physical server and the same remote deployment [see page 34] folder should be specified on each of these. Once Exclaimer Auto Responder has been installed and remote deployment options have been set, any changes made on one server can be deployed to others (each time configuration changes are saved, you are prompted to deploy them to other configured servers).

Chapter 2

The Exclaimer Console

Introduction

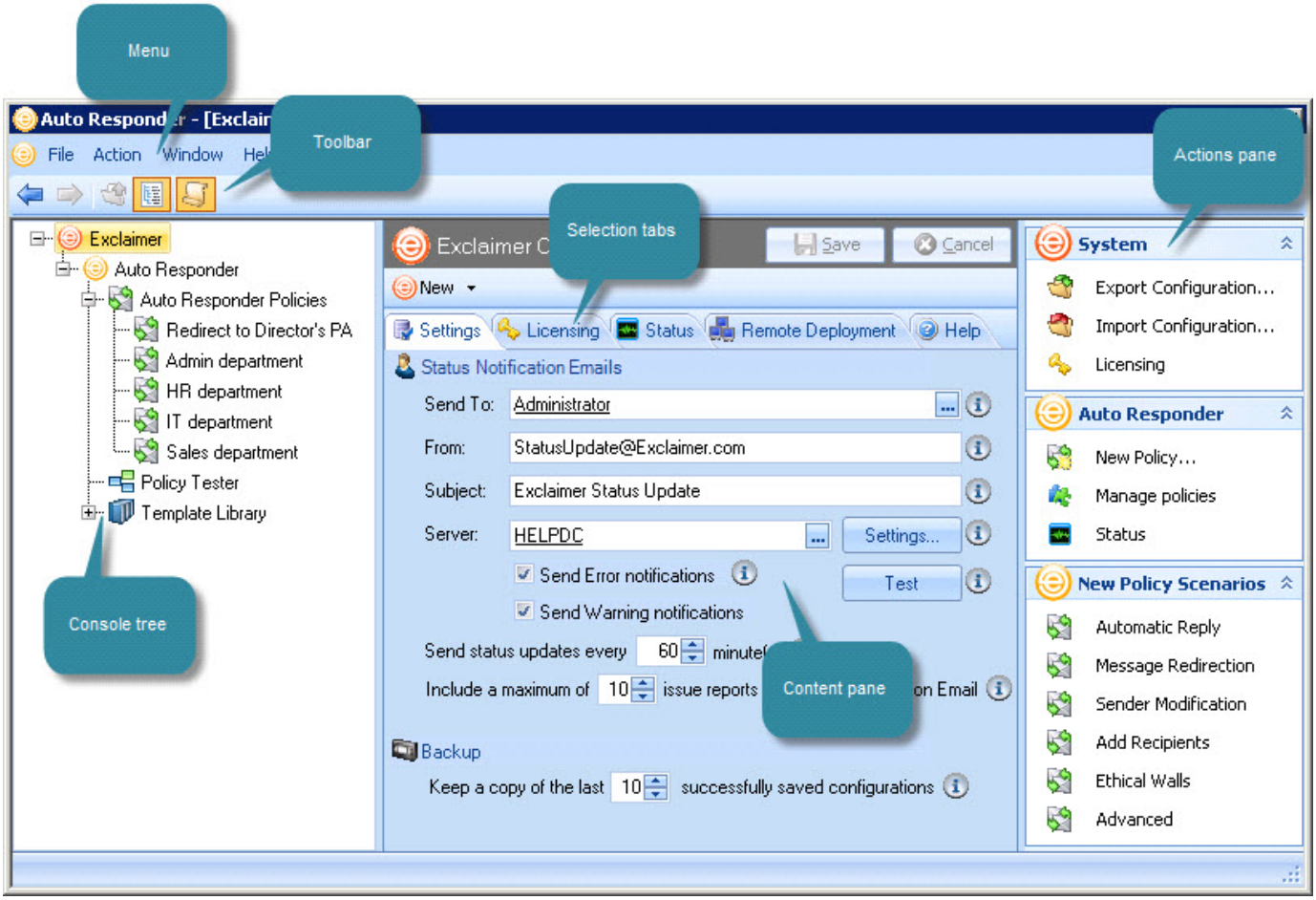
The Exclaimer console can be thought of as the 'control centre' for Auto Responder. From here, you can define general settings which are applicable to the system as a whole, and access each section of the application. This section explains how the Exclaimer console is used, including:

- Understanding the Exclaimer Console window [see page 17]
- Exclaimer console settings [see page 23]
- Exclaimer console licensing [see page 27]
- Exclaimer console status [see page 30]
- Remote deployment [see page 34]
- Exporting configuration settings [see page 39]
- Importing configuration settings [see page 39]

If you already know about the console and wish to get started with Exclaimer Auto Responder, see the working with Auto Responder section of this guide on page 57.

Understanding the Exclaimer Console Window

The Exclaimer console window is split into three panes, as shown and summarized [see page 17] below:



Exclaimer Console Summary

Available options in the Exclaimer console are summarized in the following sections:

- Console menu [see page 18]
- Console toolbar [see page 19]
- Console tree [see page 20]
- Content pane [see page 20]
- Selection tabs [see page 21]
- Actions pane [see page 21]

The Console Menu

The console menu provides access to key areas and tasks within the Exclaimer Console. Available options are summarized below:

Menu	Summary
File	**Save** Use this option to save any changes made in the content pane [see page 20]. **Exit** Use this option to close the console. If any unsaved changes are detected, you are prompted to save before exiting.
Action	Options on this menu vary, depending on which branch of the console tree [see page 20] is currently selected. Those listed below are available when the top level (Exclaimer) branch is selected: **New** Use this option to access the new auto responder policy option and create a new policy [see page 99]. **Export Configuration...** Use this option to export current configuration settings [see page 39] for the console (for example, if you wish to use the same settings to set up another server within your organization). **Import Configuration...** Use this option to import current configuration settings [see page 39] for the console (for example, if you are setting up a server using the settings from another server within your organization).
Window	**New Window** Use this option to open another instance of the console - for example, if you need to refer to settings made in one tab whilst updating another. All open windows are listed at the bottom of the window menu, so you can easily switch between sessions. The new window option is also available from the actions menu. **Cascade** If you have used the new window option to open multiple instances of the console, use this option to display all windows in a 'cascade'. **Tile Horizontally** If you have used the new window option to open multiple instances of the console, use this option to display all windows horizontally, across the screen.
Help	**Contents** Use this option to open the help system. **About** Use this option to display version information for the console.

The Console Toolbar

The console toolbar provides quick access to key tasks. These tasks are also available from the console menu [see page 18], but have been placed on the toolbar for faster access.

Options on this toolbar vary, depending on which branch of the console tree [see page 20] is currently selected. Those listed below are available when the top level (Exclaimer) branch is selected:

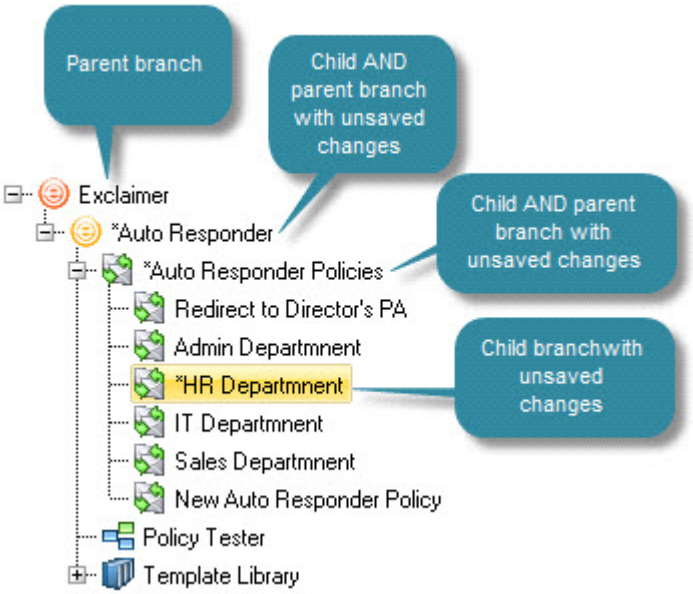
Option	Function	Summary
	Back	Whilst navigating through the console tree, use this option to go back one level.
	Forward	If you are navigating the console tree and used the back button, use this option to go forward again (i.e. to return to the point reached before you went back).
	Up	Whilst navigating through the console tree, use this option to move up to the parent of the current branch.
	Show /Hide Console Tree	Use this toggle option to show the console tree if it is currently hidden, or hide the console tree if it is currently shown.
	Show /Hide Actions Pane	Use this toggle option to show the actions pane if it is currently hidden, or hide the actions pane if it is currently shown.

The Console Tree

To navigate the Exclaimer console (and all applications within it), a familiar tree structure is used. The Exclaimer console is always at the topmost level, from which any number of parent / child branches (also known as nodes) is displayed.

Having selected a node from the tree, the content pane displays information and options that are relevant for that node. Options on the toolbar [see page 19] can be used to quickly navigate between branches within the console tree.

When a branch is selected and changes are made but not saved, the branch is displayed with an asterisk (*) symbol; you will see this at parent level (indicating that the branch contains child branches with unsaved changes) and also at child level:



The asterisk symbol is cleared from a branch once its settings have been saved.

> The console tree can be hidden or shown using the **hide / show** console tree button on the toolbar. For quick navigation, use **back**, **forward** and **up** buttons from the toolbar.

The Content Pane

Having selected a node in the console tree, any information and settings associated with that node are displayed in the content pane. These settings are accessed using a series of selection tabs [see page 21] at the top of the pane.

Selection Tabs

Information and settings are organized into a series of tabs, accessed from the top of the content pane. Available tabs vary, depending on which branch of the console tree is currently selected.

Those shown at the start of this section are available when the top level (Exclaimer) branch is selected (settings [see page 23], licensing [see page 27], status [see page 30] and remote deployment [see page 34]).

The Actions Pane

The actions pane displays quick access to common tasks, as summarized below:

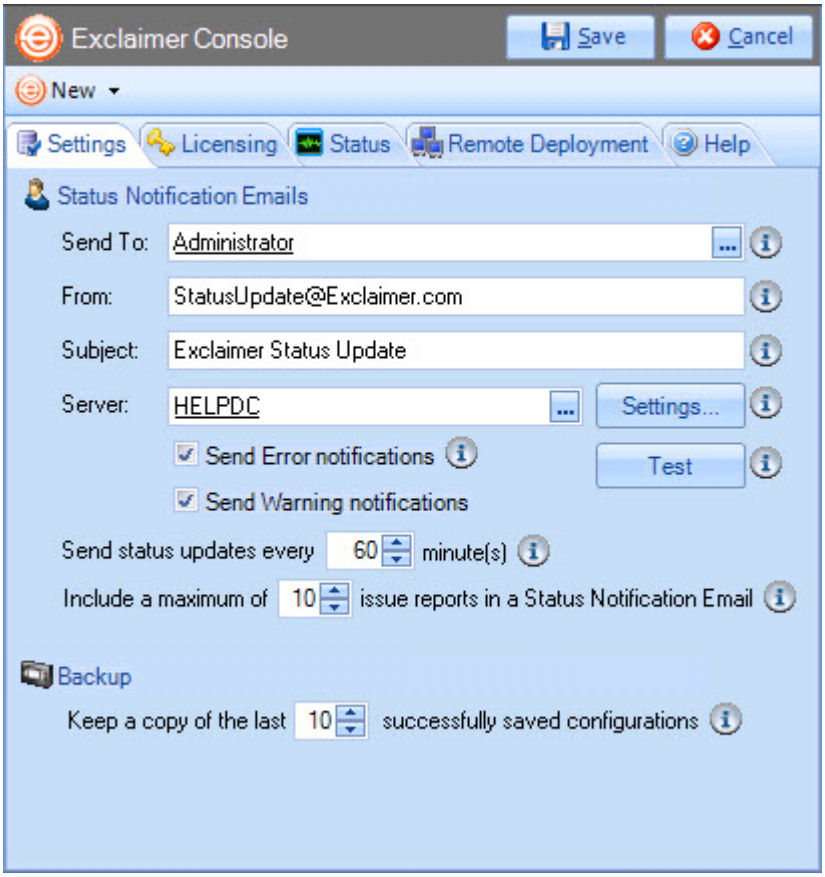
Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... [see page 39] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [see page 39] page.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.

Action	Select this option to...
New Policy Scenarios (continued)	
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

The **actions** pane can be hidden or shown using the **hide / show** actions pane button on the toolbar.

Exclaimer Console Settings

The settings tab contains options and actions [see page 25] for defining how system warning notifications are sent and received, together with backup details:

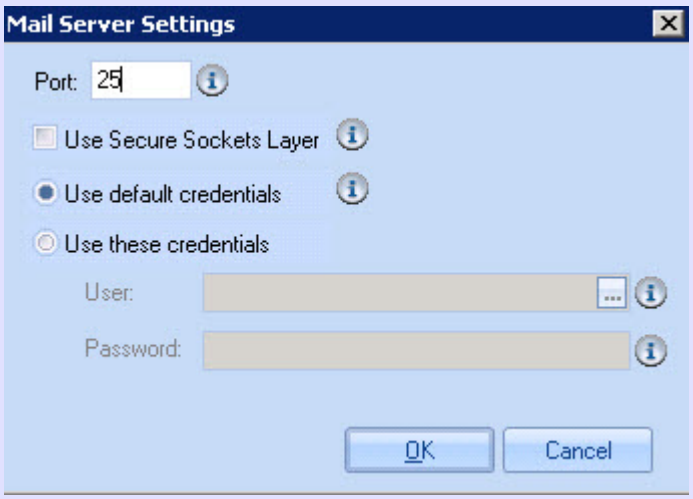


Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs.

Fields on this tab are summarized below:

Option	Summary
Status Notification Emails	
Error and/or warning messages can be sent by email. Settings in this section allow you to define who should receive these messages, and how they will be received.	
Send to	Specify an email account to receive notification emails.
From	Specify an email account to be displayed as the sender of notification emails.
Subject	Specify a subject line for notification emails.

Option	Summary
Status Notification Emails (continued)	
Server	Click the browse button - ... - to select a mail server via which email notifications will be sent. This mail server must be configured to receive SMTP email from this computer. Click the settings button to define settings for the selected mail server:



Port	Select the port number on which your mail server listens for email send requests. Typically, this is set to 25.
Use Secure Sockets Layer	Choose whether your mail server requires an SSL connection for email send requests. Typically, this is set to off.
Use default credentials / Use these credentials	Choose whether your mail server requires secure credentials in order to send emails. If you set this to on, a user and password must be specified in subsequent fields.
User	Your mail server will use credentials of the specified user when sending emails.
Password	Specify the appropriate password for the user specified for sending emails.

Send error notifications	This option must be enabled in order that notification messages can be sent.
Send warning notifications	This option must be enabled in order that warning messages can be sent.
Send status updates...	Specify the frequency with which notification emails are sent to the specified account. The frequency is entered in minutes, and must be set to a value between 1 and 1440 (one day). Notification emails are sent after the specified time has elapsed, but notification emails are not sent if no errors or warnings have been generated.

Option	Summary
Status Notification Emails (continued)	
Include a maximum of...	Specify the maximum number of errors / warnings to be included in each notification email. If the number of errors / warnings exceeds this value, only the earliest occurrences are included. A number between 1 and 99 may be entered.
Backup	
Each time that configuration changes are saved, a backup of the previous configuration is created (the location of these backup files can be found by checking the status [see page 30] tab).	
Keep a copy of the last...	Specify the maximum number of backups that will be retained, or set this value to zero if you do not wish such backups to take place.

Actions

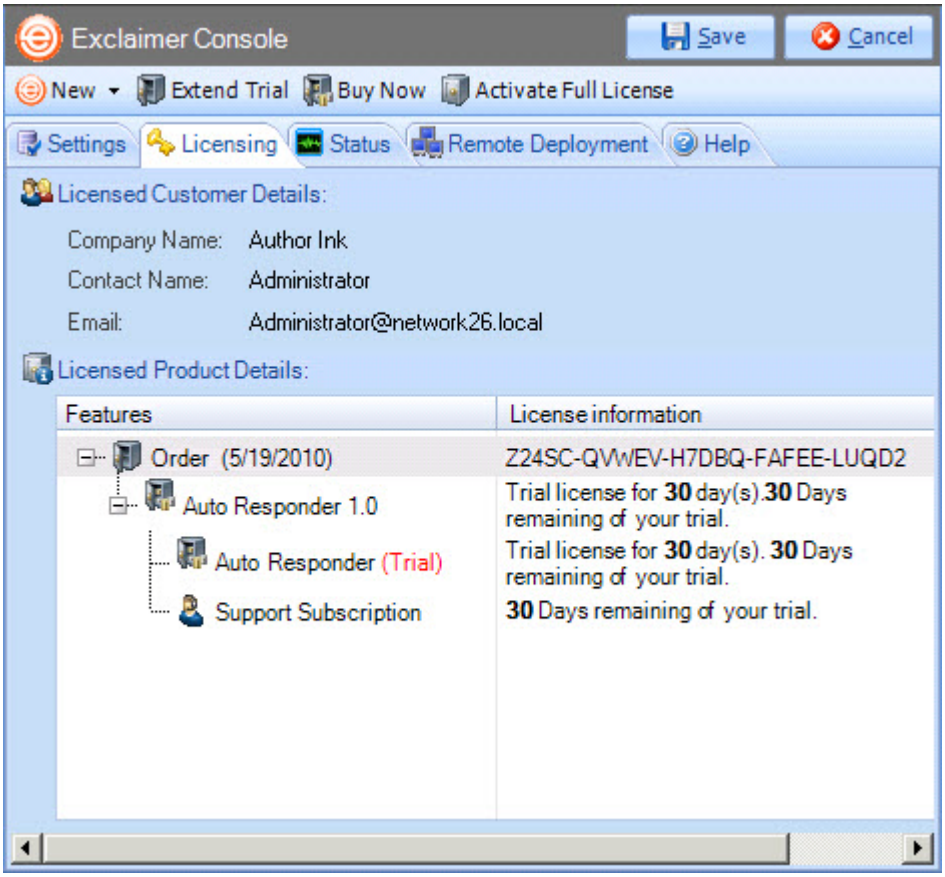
The following actions are available from the settings tab:

Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... section on page 39.
Import configuration...	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.

Action	Select this option to...
New Policy Scenarios (continued)	
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Exclaimer Console Licensing

The licensing tab contains information and actions [see page 29] regarding licenses for Auto Responder:



Licensing information is summarized in the following sections:

- The licensing process [see page 28]
- Licensing information [see page 28]
- The licensing toolbar [see page 28]
- Actions [see page 29]

The Licensing Process

Our aim is to get you working with Exclaimer software as quickly as possible, with minimal restrictions. As such, we have implemented a flexible licensing policy. If you have installed Exclaimer software for the first time, you can use it for five days without any form of registration. After five days, you are prompted to register for a 30 day trial. Having completed this trial, you can:

- Purchase the product from the Exclaimer website or by contacting the Exclaimer sales team.
- Contact the Exclaimer sales team to extend your trial.

Licensing Information

The licensing tab shows any contact details associated with this Exclaimer license, together with installed products, features and version information. You can also see the type of license that is currently in place and the license status (for example, the number of days remaining for a trial period).

The Licensing Toolbar

When the licensing tab is displayed, the licensing toolbar contains the following options:

Toolbar Option	Summary
New > Auto Responder policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy.
Register for 30 day trial	Before using this software, you must register your installation of the Exclaimer Console and its associated products. Click this option to open the register for 30 day trial wizard and follow on-screen instructions to register your trial.
Extend trial	This option is only displayed if you have registered for a 30 day trial. To extend a trial, use the extend trial button and note information required, then contact the Exclaimer sales team using contact details provided. Once your trial extension has been confirmed, continue with the licensing wizard to activate the extension.
Buy now	Access the Exclaimer website products page to purchase a license.
Activate full license	Having purchased a license, you will receive an email which includes a product activation key. Use the activate full license option to activate your license.

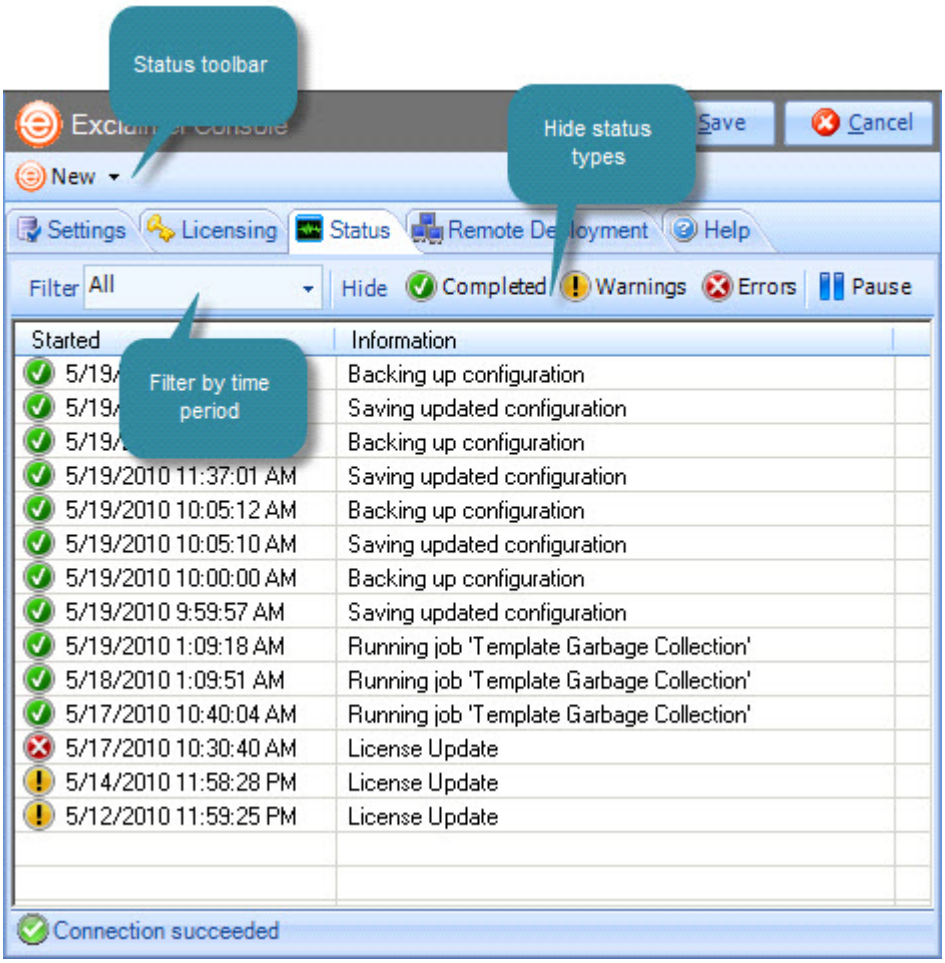
Actions

The following actions are available from the licensing tab:

Action	Select this option to...
System	
Export configuration	Export all settings and policies - see the export configuration... section on page 39.
Import configuration	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Exclaimer Console Status

The status tab contains information and actions [see page 32] regarding activity within the Exclaimer console. Double click an entry in the list to view further details. Entries are categorised as completed, warnings or errors, as shown below:



Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

Available options are summarized in the following sections:

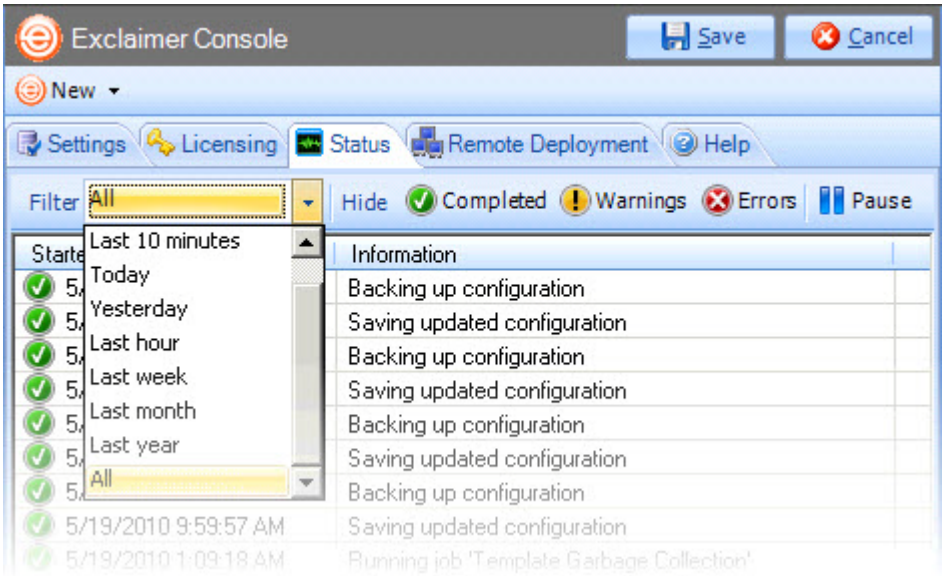
- Filtering the status list [see page 31]
- The status toolbar [see page 32]
- Actions [see page 32]

Filtering the Status List

Potentially, the status list could become very long; therefore it is useful to filter the list to display entries that are most relevant to you. Options are available to filter the status list by a given time period and/or by category.

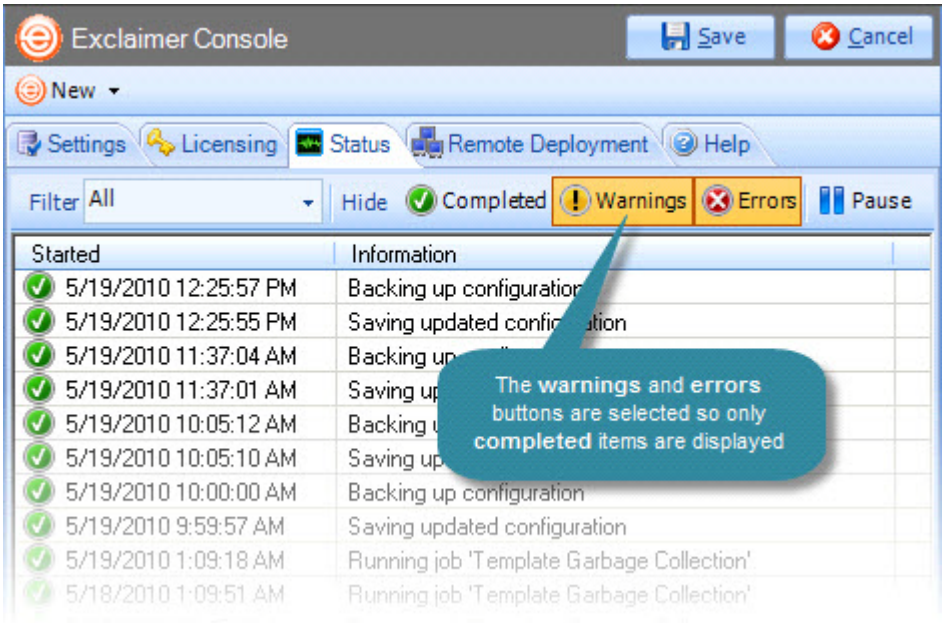
Filter by Time Period

Use the drop-down filter list to select a time period. Having made your selection, the status list is updated to show only items that occurred within that time period:



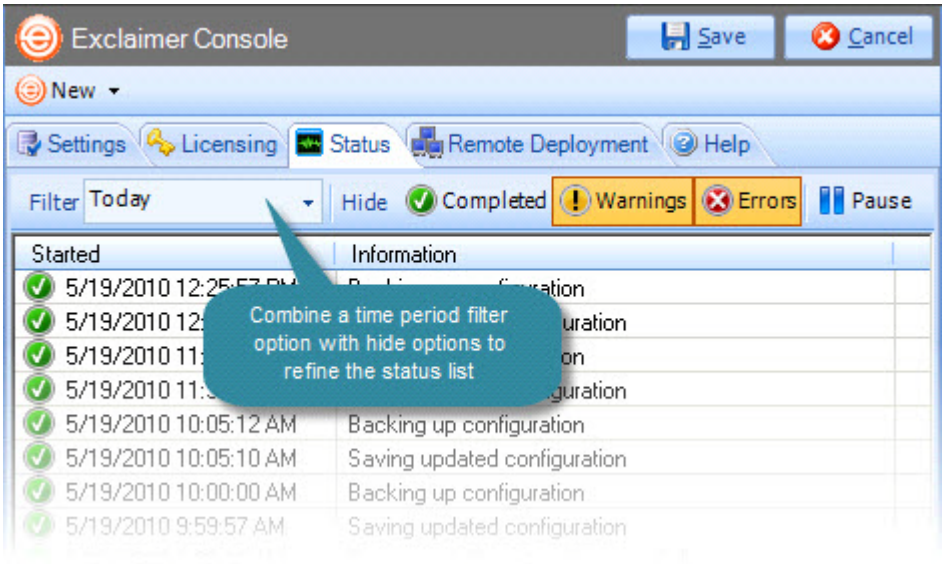
Filter by Status Type

Use hide buttons to exclude items for completed, warnings or errors from the list. For example, to exclude all items except for those in the completed category, you would click hide buttons for warnings and errors categories:



Filter by Time Period and Category

For maximum flexibility, you can refine the status list using both filter and hide options:



The Status Toolbar

When the status tab is displayed, the status toolbar contains the following options:

Toolbar Option	Summary
New > Auto Responder policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).

Actions

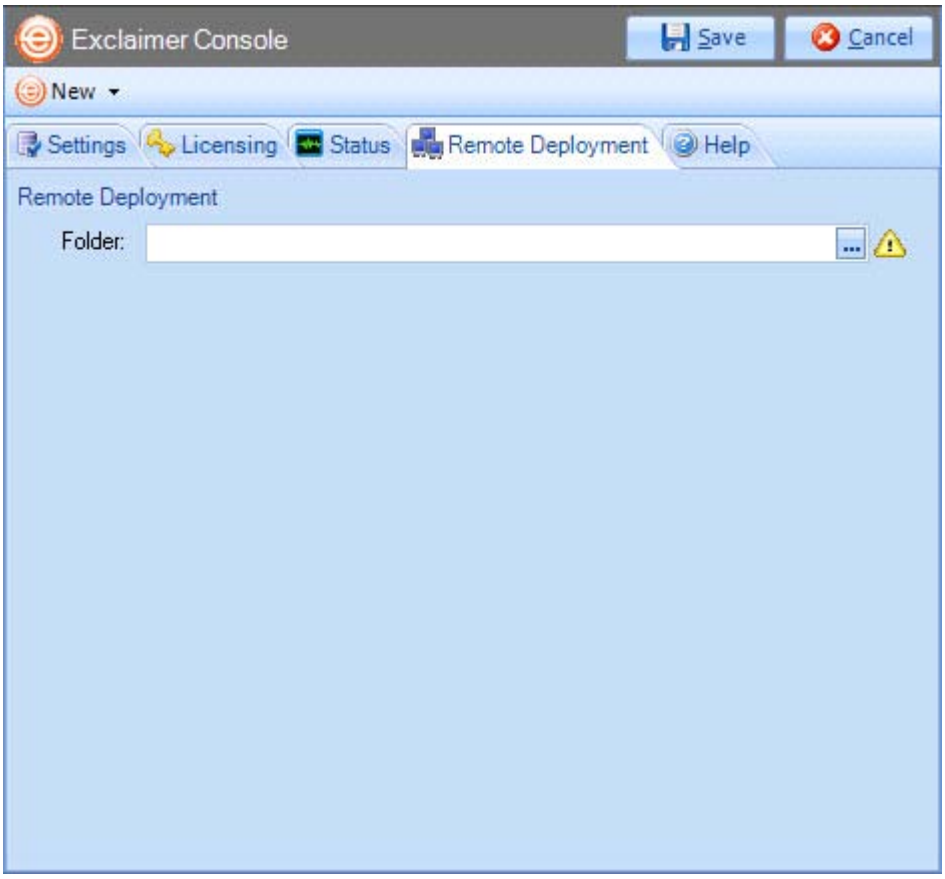
The following actions are available from the status tab:

Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... section on page 39.
Import configuration...	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).

Action	Select this option to...
Auto Responder (continued)	
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Remote Deployment

If you have multiple Exclaimer installations on your network (for example, you might have servers in different offices around the country), you can manage configuration in a single location and deploy this to all other servers. To do this, use the remote deployment tab to specify a shared location:



Whenever you save any changes to the configuration, you are asked to confirm if you would like to deploy them to other servers. If you opt to deploy changes, a file is written to the remote deployment folder and imported by the other installations.

Initially, Exclaimer software must be installed on each server - installation cannot be completed via remote deployment. Once installed, specify a **remote deployment** folder to manage subsequent configuration changes with remote deployment (each installation must have the same **remote deployment** folder).Alternatively, use the **cancel** button to abandon all changes.

How it Works

The remote deployment folder is defined using the remote deployment tab within the Exclaimer Console. Please refer to the help file (within Auto Responder) for further information about this tab.

The specified folder must be a shared folder on the network (only one remote deployment folder should be used on an entire domain). When configuration changes are saved, the computer (on which those changes have been saved) pushes new configuration data to the remote deployment folder.

Remote machines receive notification from the operating system when new configuration data is detected in the shared folder, and they then pull (i.e. import) that data into their local installation. Push and pull operations are completed via the Exclaimer Remote Deployment service.

The Remote Deployment Folder

Create a shared folder on your network that will be accessible by all machines that are running Exclaimer Auto Responder.

If you do not want the share to be visible to users, you should use a hidden share. This is done by adding a dollar ($) symbol to the end of the share name. Hidden shares cannot be viewed when browsing the network with Explorer, for example.

Ensure that the user who is logged into the Exclaimer console (that is saving data) has Read and Write access to this folder.

The following sections detail two methods of applying folder permissions. These are applicable for both the Sharing and the NTFS Security permissions of the shared folder - i.e. you must make the same permission changes in both the Sharing and Security tabs of the folder's properties dialog.

Folder Permissions (Easy Method)

Allow the Everyone group to have Read permissions.

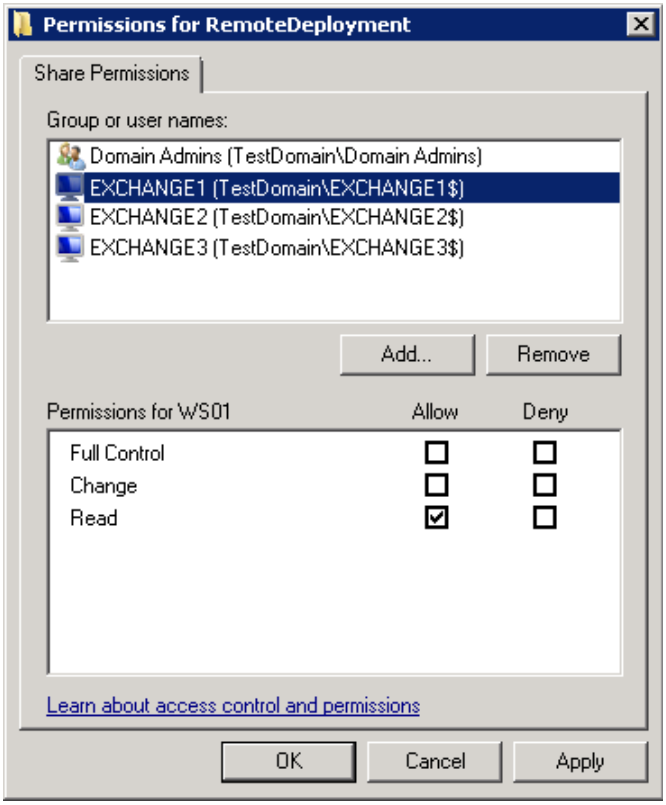
Folder Permissions (Secure Method)

Allow Read permissions only for the computer account of each server with Exclaimer Auto Responder installed upon it.

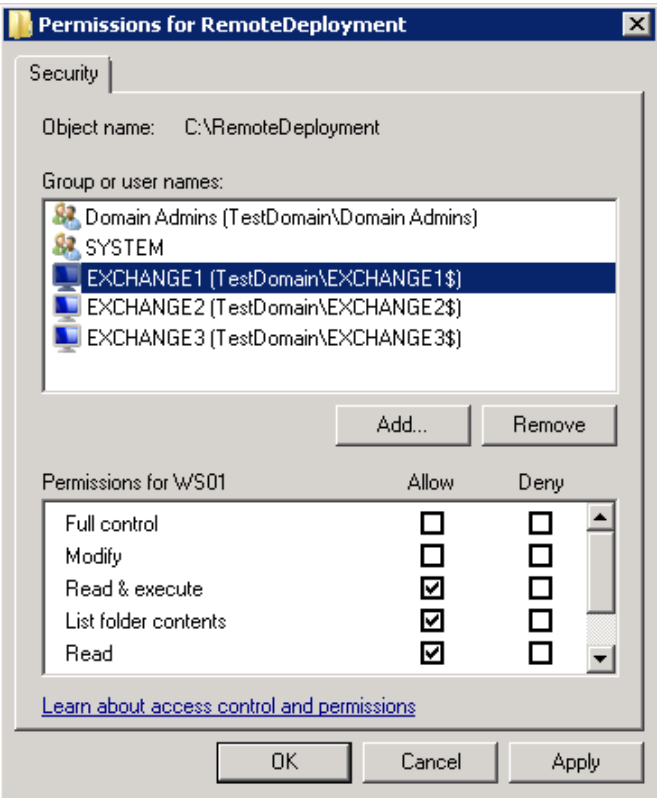
This is essential because the remote deployment service runs under the LocalSystem account; this account (as the name suggests) only has access to the local system of the machine that it is running on, not to any network resources.

The only way this account can ever see a network resource is when the computer account is given specific access to that resource – i.e. the folder on the network resource allows itself to be accessed by the LocalSystem account of a specific remote machine. In this case, access is restricted to only reading data from the remote deployment folder.

Example permission settings are shown below:



Share Permissions Tab



Security Permissions Tab

Remote Deployment Timings

As soon as the Exclaimer Remote Deployment service notices that there has been a change to the remote deployment folder, it starts a timer. Every ten seconds a check is made to see if the file has been written to in the last five seconds. If it has not, the file is added to a queue which will perform the actual import; otherwise the file remains in the timer list.

This means that the import should begin a maximum of ten seconds after the save finishes, though in practice it could be a little more than this depending on server load and how quickly the import thread is given control by the operating system. Similarly, the import could begin sooner, depending on when the save completes relative to the timer interval.

Before checking that configuration changes have been applied successfully on remote machines, sufficient time should be allowed for those machines to actually perform the import (the import can take some time with complex configurations).

Changing an Existing Remote Deployment Folder

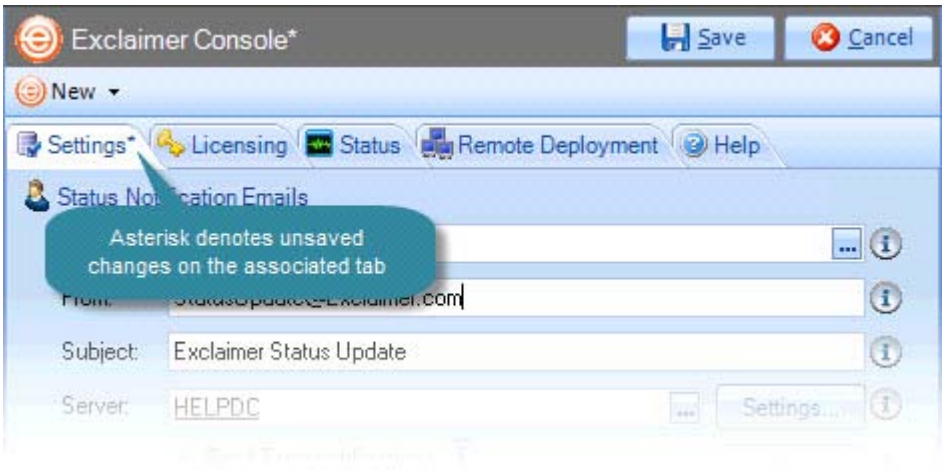
If all Auto Responder installations are set to point to a specific remote deployment folder and you later decide to change that folder, there is no need to manually change every server to point to the new location.

Having changed the location on one machine and saved the configuration, that machine will write a copy of the configuration data to both the old AND the new locations. Any servers pointing to the old location will import the configuration which includes the new remote deployment folder path so, on subsequent deployments, they will pull data from the new location.

As such, you are advised NOT to delete the old remote deployment folder until enough time has elapsed for all remote machines to import the configuration file that contains the new folder location.

Saving Changes in the Exclaimer Console

If a tab contains any unsaved changes (irrespective of which branch in the console tree [see page 20] is active), it is displayed with an asterisk (*) symbol - for example:



Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the save button to save changes across all tabs.

Before changes are saved, existing configuration settings are automatically backed up; you can find the location of this backup file by checking the status tab [see page 30] for the Exclaimer console.

If you are unsure about any changes that have been made, use the cancel button to abandon all changes.

Exporting Configuration Settings

The export current configuration settings option is used to export all settings for the Exclaimer console, and all Exclaimer applications within it. As such, the export will include all settings, policies [see page 49] and templates [see page 164] for Exclaimer Auto Responder.

The export process writes all settings to an econfig file; this is a proprietary file type for Exclaimer products and is required if you wish to import settings from a file. To export current settings, follow the steps below:

1. Ensure that Exclaimer is selected in the console tree (i.e. the topmost branch)
2. Select export current configuration settings from the actions pane, or from the action menu. The export configuration window is displayed.
3. Navigate to the required drive and folder, into which the export file should be saved.
4. Enter the required file name for the export file.
5. Click save to complete the export.

Importing Configuration Settings

The import current configuration settings option is used to import all settings for the Exclaimer console, and all Exclaimer applications within it. As such, the import will include all settings, policies [see page 49] and templates [see page 164] for Exclaimer Auto Responder.

Settings must be imported from an econfig file; this is a proprietary file type for Exclaimer products, and is created whenever the export configuration settings [see page 39] option is used. To import configuration settings, follow the steps below:

1. Ensure that you have backed up existing settings by exporting the current configuration [see page 39].
2. Ensure that Exclaimer is selected in the console tree (i.e. the topmost branch).
3. Select import current configuration settings from the actions pane, or from the action menu. The import configuration window is displayed.
4. Navigate drives and folders to select the econfig file to be imported.
5. Click open to complete the import.

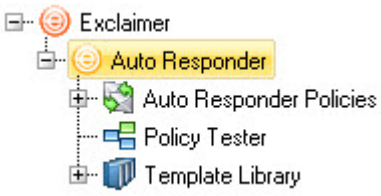
Remember that **all** settings will be imported, which means that your existing configuration will be overwritten. Before the import takes place, existing configuration settings are automatically backed up; you can find the location of this backup file by checking the status tab [see page 30] (see page 25) for the Exclaimer console. Alternatively, use the cancel button to abandon all changes.

Chapter 3

General Settings & Information for Auto Responder

Introduction

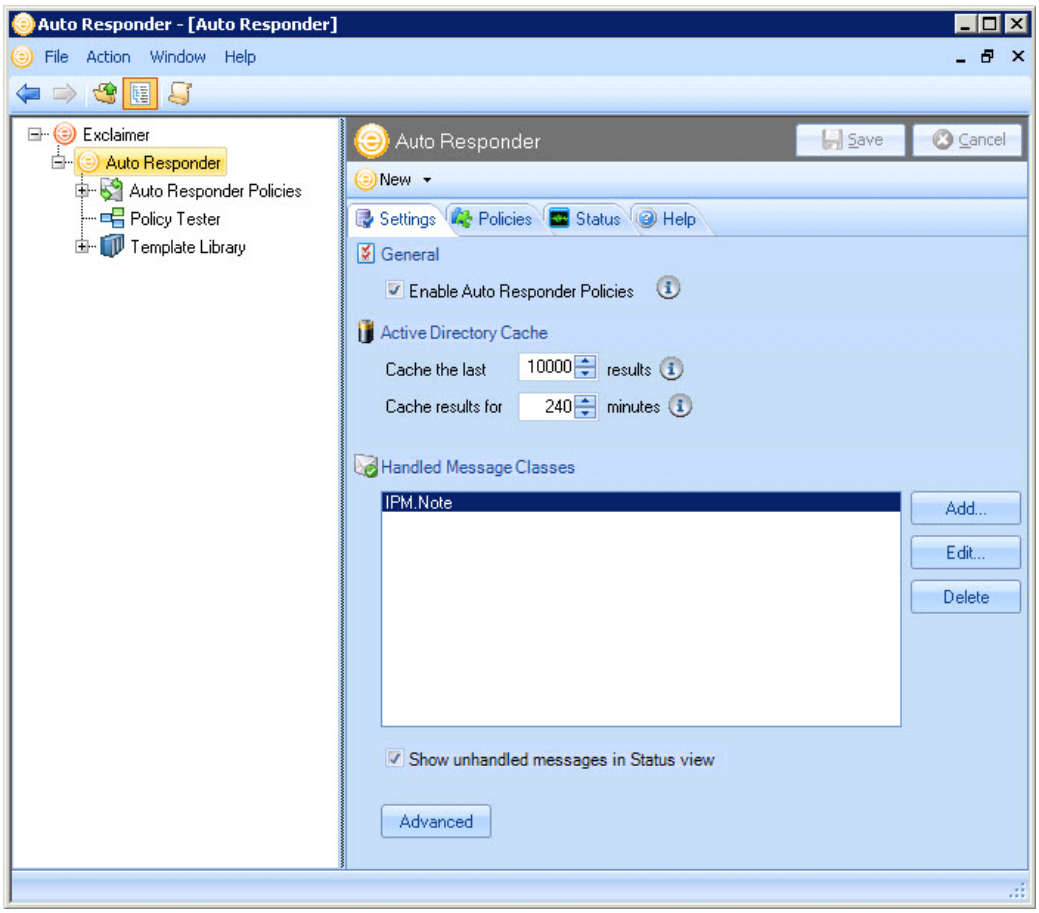
The Auto Responder branch (within the Exclaimer console [see page 16] tree) is where all setup is completed:



When the parent branch (Auto Responder) is selected, general settings and information [see page 41] can be viewed and updated. Below this, three child branches are used to access the three main elements of Exclaimer Auto Responder:

- Auto Responder policies [see page 57]
- The policy tester [see page 152]
- The template library [see page 164]

When the parent branch (Auto Responder) is selected (within the Exclaimer console [see page 16]), general settings and information can be viewed and updated:



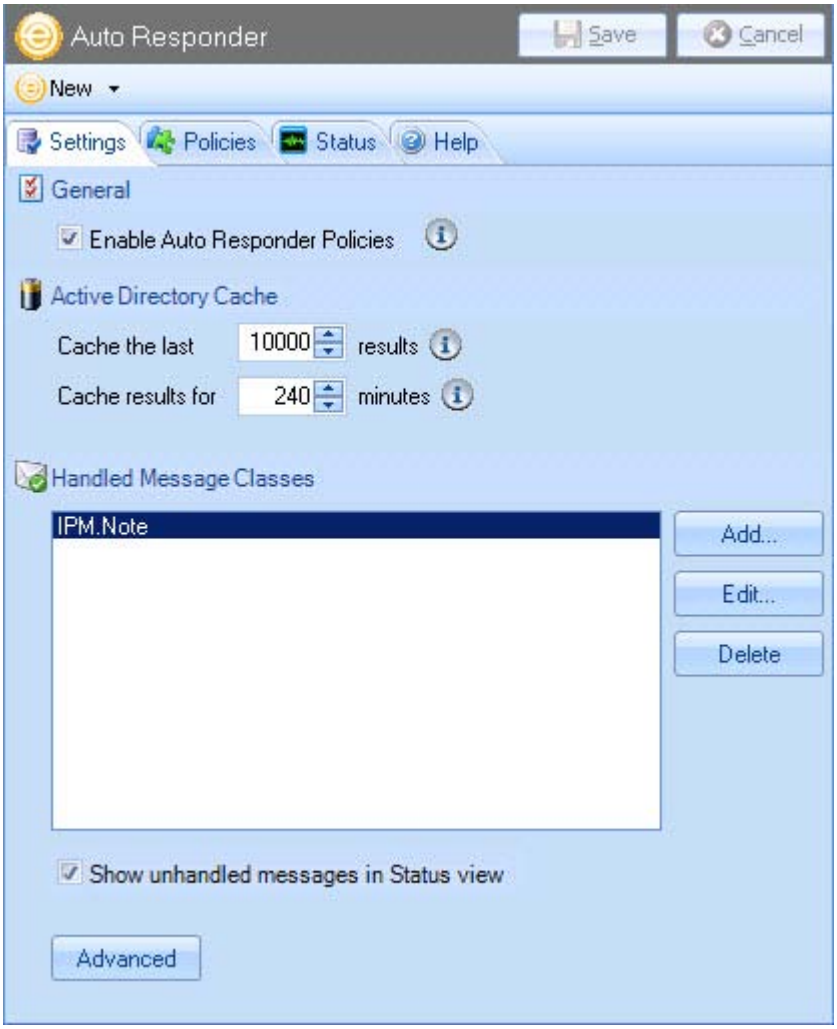
From here, you can:

- Update general settings [see page 43] from the settings tab
- View existing policies [see page 49] from the policies tab
- View status information [see page 53] from the status tab
- Add a new policy [see page 99] via toolbar or actions pane options

For further information about the Exclaimer console (including the menu, toolbar and actions pane), see understanding the Exclaimer console window on page 17.

Auto Responder Settings

The settings tab contains general settings for Auto Responder:



Available options are summarized in the following sections:

- Available settings [see page 44]
- Advanced settings [see page 45]
- The settings toolbar [see page 47]
- Actions [see page 47]

Available Settings

Fields on this tab are summarized below:

Option	Summary
Enable Auto Responder policies	Enable or disable all Auto Responder policies. If this option is not set to enabled, Auto Responder policies will **not** be applied to your organization's email messages.
Cache the last...results	To optimize performance, Exclaimer caches information from your Active Directory. Use this field to specify the maximum number of items to cache; we advise setting this field to the number of people within your organization plus 10%, up to a maximum of 50,000.
Cache results for...minutes	This figure specifies the frequency with which the Active Directory cache is recreated. A higher number (greater than 240) means that the cache is created less frequently. This means that it takes longer for Active Directory changes to be reflected within Auto Responder, however system performance is greater as a result. Conversely, a lower number (less than 240) means that the cache is created more frequently, thus changes are reflected in Auto Responder more quickly, but system performance may be slower.
Handled message classes	This section determines the type (class) of messages that will be handled by Auto Responder. By default, the class for email messages (IPM) is defined and under typical circumstances, this is sufficient. However, some organizations may wish to send automated replies to other types of Outlook items - for example, to meeting requests or calendar appointments. If you wish to apply Auto Responder to other items, use the **add** option to add the relevant class.
Show unhandled messages in status view	Select this option to report unhandled messages in the status tab [see page 53].

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

Advanced Settings

Click the advanced button on the settings tab to access additional settings for fault tolerance and diagnostics, as summarized below.

Fault Tolerance

For some organizations, auto responses can be critical - to the extent that the Microsoft Exchange server must be stopped in the event of a problem with Auto Responder. For others, it is sufficient to quarantine messages but still send messages (where applicable).

The fault tolerance tab allows administrators to specify how messages should be handled in the event of a fault during message processing. These options are summarized below:

Option	Summary
When a fault is encountered during the processing of a message	
Deliver the message anyway	In the event of a fault, deliver the message at whichever point it got to through Auto Responder processing and do not take a quarantine copy. In this situation, the only indication that something went wrong would be an error on the status [see page 53] page.
Quarantine the message (do not deliver)	In the event of a fault, quarantine the message and do not attempt delivery.
Quarantine the message (but deliver the original)	In the event of a fault, quarantine the message and deliver the message in its original form. In this situation, a copy of the message is stored in the quarantine folder for later analysis, and the message is sent at whichever point it got to through processing.
If quarantine fails	
Deliver the message anyway	If a quarantine setting is selected but quarantine is not possible at the time of a fault, deliver the message anyway.
Stop the Microsoft Exchange Transport Service	If a quarantine setting is selected but quarantine is not possible at the time of a fault, stop the Microsoft Exchange Transport Service so that all incoming and outgoing messages are stopped. To apply this setting, account credentials must be provided for a user with appropriate permissions to stop this service.
Quarantine will fail if there are more than xx messages in the quarantine folder	Use this option to specify a number of messages to be quarantined before quarantine fails and any 'if quarantine fails' actions come into force.
Folder	Use the browse button to select a folder in which quarantined messages are stored.

Option	Summary
If quarantine fails (continued)	
Notify sender of the action taken	Select this option to notify the sender of action taken with their message in the event of a fault.
Notify Exclaimer administrator	Select this option to notify the Exclaimer administrator of action taken with their message in the event of a fault. The email address used will be that defined during the Exclaimer installation/configuration [see page 12].

Diagnostics

A diagnostics email is only used by Exclaimer support, in the event of a query. It contains information about particular emails, including system information, the email message before and after processing, status information and a copy of the user's control file.

This option should not be enabled unless you are asked to do so by Exclaimer support. These options are summarized below:

Option	Summary
Enable diagnostics	Select this option to enable diagnostics.
Diagnostic Recipients	Use the browse button to select people who should receive the diagnostics email.
Attachment Extension	Some diagnostic information is sent as an attachment with the diagnostics email. This is a standard extension to apply to all attachments (this can be useful - for example - to stop diagnostic emails being blocked by anti-virus and anti-spam applications).
Match Sender	The sender of the messages to be matched for diagnostics emails.
Match Subject	The subject of the messages to be matched for diagnostics emails.
Match Recipients	The recipient of messages to be matched for diagnostics emails.

The Settings Toolbar

When the settings tab is displayed, the settings toolbar contains the following options:

Toolbar Option	Summary
New > Auto Responder policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy.

Actions

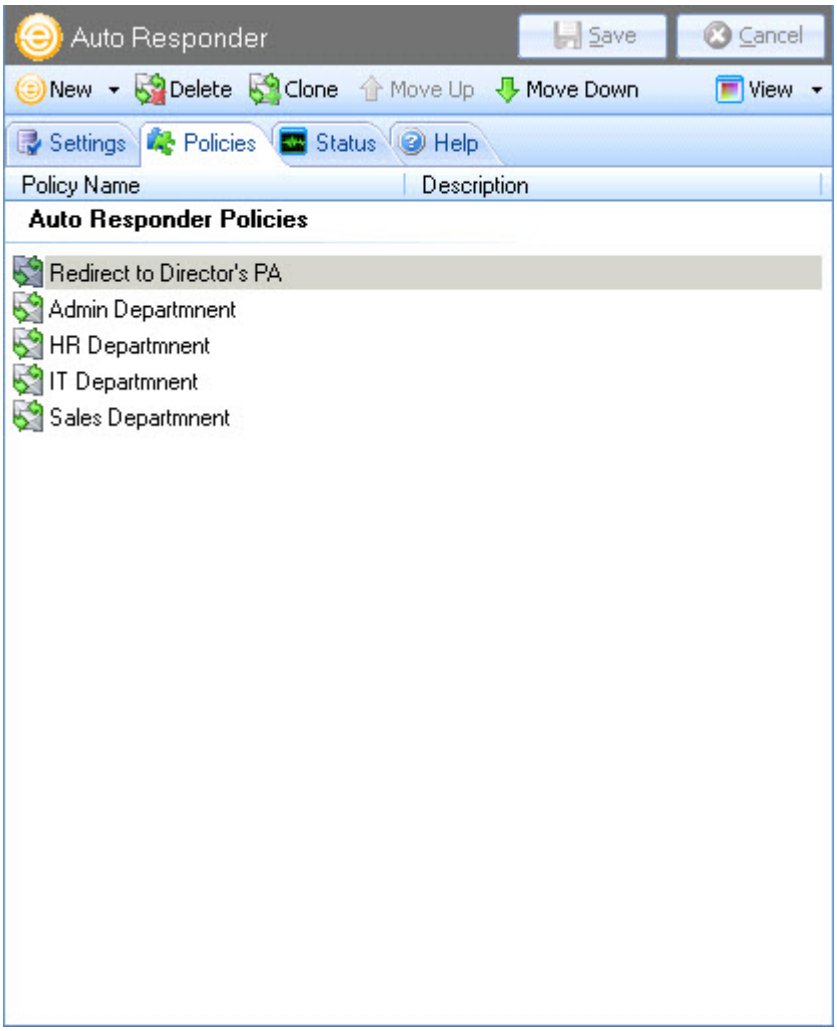
The following actions are available from the settings tab:

Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... section on page 39.
Import configuration...	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.

Action	Select this option to...
New Policy Scenarios (continued)	
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Auto Responder Policies

The policies tab contains quick access to existing policies and options for completing key tasks relating to policies:

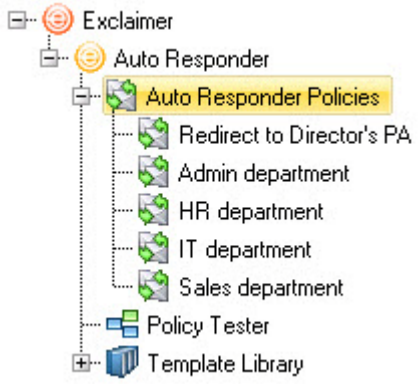


It is important to note that policies are processed in the order that they are listed here. You can use move up / move down [see page 50] options to change the sequence of this list, and use next policy [see page 98] options for greater control over processing sequence. Available options are summarized in the following sections:

- The policy list [see page 50]
- The policies toolbar [see page 50]
- View options [see page 51]
- Actions [see page 52]

The Policy List

All existing policies are listed in the main content area; these are the same policies that you will see listed in the console tree:



It does not matter if you access policies from the console tree, or from the policy list - use whichever method is most convenient for the task in hand.

The Policies Toolbar

When the policies tab is displayed, the policies toolbar contains the following options:

Toolbar Option	Summary
New > Auto Responder policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy.
Delete	Use this option to remove [see page 130] the currently selected policy. Select a policy from the list and use this option to delete it - the policy is removed from the list but is only permanently deleted when changes are saved [see page 38].
Clone	If you need to create a policy which is similar to an existing policy, use this option to clone [see page 128] (duplicate) the existing policy and then edit [see page 129] the duplicate version as required (this can be much quicker than creating a new policy from first principles).
Move Up / Move Down	Use these options to reorganize the policy list and determine the order in which policies are applied. Select a policy and click move up or move down as required.

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

View Options

The view option can be used to determine whether policies are displayed in list (details) form...

... or as large icons:

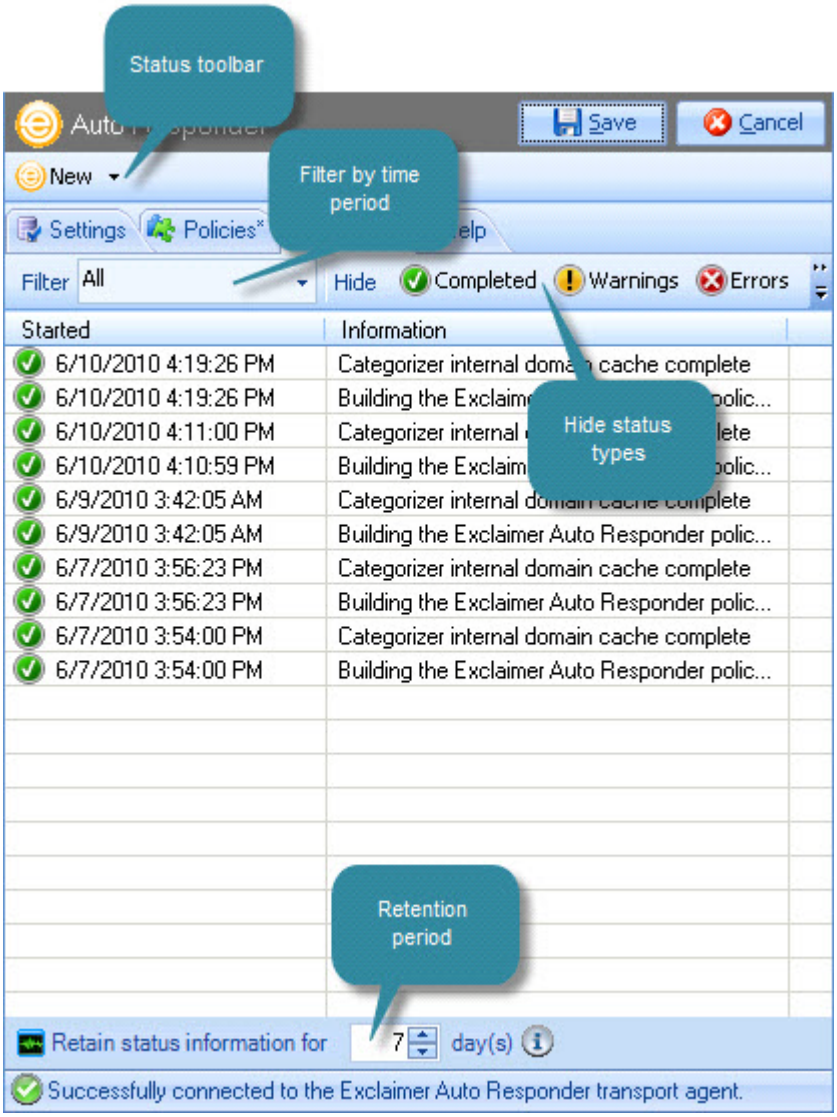
Actions

The following actions are available from the settings tab:

Action	Select this option to...
System	
Export configuration	Export all settings and policies - see the export configuration... section on page 39.
Import configuration	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
New Policy Scenarios (continued)	
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Auto Responder Status

The status tab contains information and actions [see page 55] regarding activity with Auto Responder policies - double click an entry in the list to view further details. Entries are categorised as completed, warnings or errors, as shown below:



Available options are summarized in the following sections:

- Filtering the status list [see page 54]
- The status toolbar [see page 54]
- Actions [see page 55]

Filtering the Status List

Potentially, the status list could become very long; therefore it is useful to filter the list to display entries that are most relevant to you. Options are available to filter the status list by a given time period, and/or by category.

Filter by Time Period

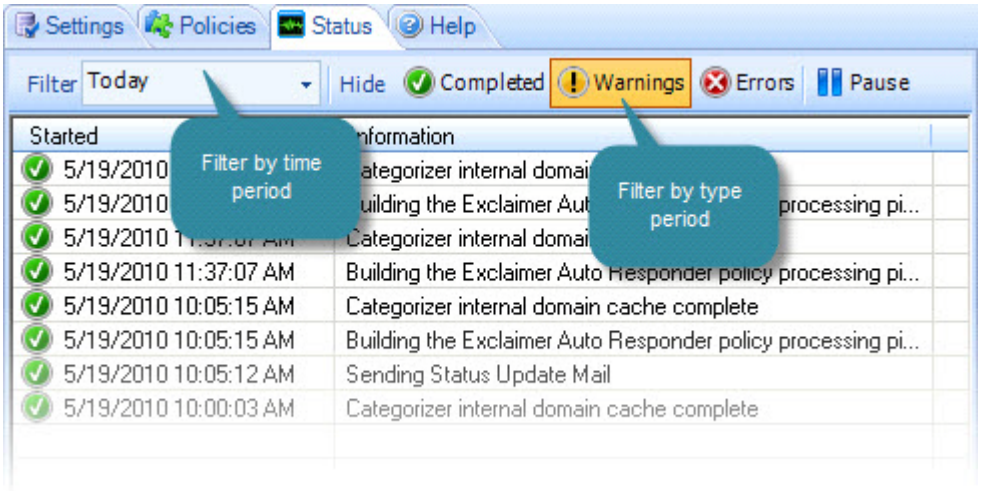
Use the drop-down filter list to select a time period. Having made your selection, the status list is updated to show only items that occurred within that time period. For more detailed information about using this feature, see the Exclaimer console status [see page 31] section of this guide.

Filter by Status Type

Use hide buttons to exclude items for completed, warnings or errors, from the list. For example, to exclude all items except for completed entries, you would click hide buttons for warnings and errors categories. For more detailed information about using this feature, see the Exclaimer console status [see page 31] section of this guide.

Filter by Time Period and Status Type

For maximum flexibility, you can refine the status list using both filter and hide options:



The Status Toolbar

When the status tab is displayed, the status toolbar contains the following options:

Toolbar Option	Summary
New > Auto Responder policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy.

Status Information Retention

At the bottom of the status tab, you can set the number of days that status information is to be retained:

Any status information older than the specified number of days is permanently deleted.

Actions

The following actions are available from the status tab:

Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... section on page 39.
Import configuration...	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.

Action	Select this option to...
New Policy Scenarios (continued)	
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

Chapter 4

Working with Auto Responder Policies

Introduction

Using Auto Responder, policies are defined to determine:

- Any automatic action(s) [see page 58] to be taken when emails are received
- The circumstances [see page 58] under which those actions are performed
- Any content [see page 58] that may be required to complete an action

These elements are summarized below.

Action(s) to be Taken

The first step in creating a new policy is to choose the policy type [see page 60]. A range of policy types are available and different actions are associated with each one.

For example, you might choose an automatic reply policy [see page 100], which automatically sends a predefined response [see page 58] when emails are received, or you might choose a message redirection policy [see page 108] which automatically sends the email to an alternative mailbox.

Circumstances under which a Policy is Triggered

For each policy, a wide range of conditions [see page 84] and exceptions [see page 91] can be specified to control the circumstances under which a policy is triggered.

For example, you might need to apply different policies for different departments within your organization, or for individual staff members, or perhaps based upon the content or subject line of messages received.

You can also use date range [see page 96] options to create policies which are only triggered at certain times and use next policy [see page 98] options to create a series of connected rules.

Content Required for an Action

Certain policy types trigger an action which requires you to provide predefined content. For example, when creating an automatic reply policy [see page 100], the content of the automated response to be sent must be specified.

This is done using templates [see page 164]; a number of standard templates are available and, if required, you can add your own using an intuitive template editor [see page 184].

This section contains information about working with policies, including:

- Accessing existing policies [see page 64]
- Policy types [see page 60]
- The anatomy of a policy [see page 72]
- Adding Auto Responder policies [see page 99]
- Cloning a policy [see page 128]
- Changing a policy [see page 129]
- Enabling and disabling a policy [see page 129]
- Removing a policy [see page 130]

You can also learn more about specific tasks, using the how to section for Auto Responder policies [see page 131].

Policy Types

The first step in creating a new policy [see page 99] is to choose the policy type. A range of policy types are available and different actions are associated with each one, as summarized below:

- Automatic reply [see page 60]
- Message redirection [see page 61]
- Sender modification [see page 61]
- Add recipients [see page 62]
- Ethical walls [see page 62]
- Advanced [see page 63]

Automatic Reply

An automatic reply policy [see page 100] can be used when you need to send an automated response to emails. For example, if you have advertised a job and are receiving a large number of applications, you may wish to send confirmation that emails have been received and are being processed.

Similarly, you might have an enquiries email address and want to send a standard response (perhaps including some company literature as attachments), or you might want a more consistent Out of Office message to be sent (and perhaps only active on certain days of the week such as weekends).

When an automatic reply policy is created, you are asked to select a template to be used as the content of the automated response. A number of standard templates are available in both HTML and plain text format but you can also add your own templates using an intuitive template editor [see page 184].

By default, settings on the original message [see page 74] tab are defined to deliver the message (without modification) to the intended recipient. Also by default, auto response [see page 78] settings are set to send the automated message from the recipient to the sender. All of these settings can be adjusted [see page 129] if required.

For further information see adding an automatic reply policy on page 100.

Message Redirection

A message redirection policy [see page 108] can be used when you need to redirect incoming email messages to an alternative mailbox. For example, you may wish to redirect all messages sent to members of a particular team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering their role.

Alternatively, you might have a domain that is being retired and want messages addressed to a user at the old domain to be re-addressed to the same user at your primary domain, or you may need to set up a catch-all policy so that all messages sent to unrecognized email addresses at your domain are redirected to a single mailbox for review.

When a message redirection policy is created, you can choose to redirect messages to an alternative email address, or to the same recipient at a different domain. By default, settings on the original message [see page 74] tab are defined to deliver the message but modify recipient(s) to the alternative address specified. Also by default, auto response [see page 78] settings are not set - i.e. no response message is sent which means that the sender is not aware that their message was redirected.

All of these settings can be adjusted [see page 129] if required. For further information see adding a message redirection policy on page 108.

Sender Modification

A sender modification policy [see page 112] can be used in cases where users need to send emails from different email addresses and therefore need the facility to control which email address appears in the ‘From’ field of any messages they send.

For example, your organization might consist of two companies, where some employees work in both, or you might have individual members of a team who log on to Outlook with their own profile, but any messages they send should appear to come from the central team mailbox.

When a sender modification policy is created, you can choose to change the sender's address to an alternative email address or domain. By default, settings on the original message [see page 74] tab are defined to deliver the message but modify the sender's address to a given alternative.

Also by default, auto response [see page 78] settings (on the auto response [see page 78] tab) are not set - i.e. no response message is sent which means that the recipient is not aware that the message originated from a different sender. All of these settings can be adjusted [see page 129] if required. For further information see adding a sender modification policy on page 112.

Add Recipients

An add recipients policy [see page 116] can be used in cases where you need to automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager, or you might want to automatically add a manager as a BCC recipient on all messages sent from a specific employee.

When an add recipient policy is created, you can choose to add recipients in the To, CC and/or BCC fields of the email message. By default, settings on the original message [see page 74] tab are defined to deliver the message but add given recipients.

Also by default, auto response [see page 78] settings are not set - i.e. no response message is sent which means that neither the sender nor recipients are aware that recipients were added automatically. All of these settings can be adjusted [see page 129] if required. For further information see adding an add recipients policy on page 116.

Ethical Walls

An ethical walls policy [see page 119] can be used to prevent prohibited email communication - for example, your organization might include two departments where a conflict of interests could arise if communication between them occurs.

When an ethical walls policy is created, you specify two constituent parts (A and B) between which email transmission will be blocked. For example, you might define A as all users within the finance department and define B as all users within the trading department.

If required, you can choose to notify the original sender and /or recipients and / or other parties when an email between the two specified parties is attempted and blocked. The content of this notification message is defined in a template [see page 164]; a number of standard templates are available in both HTML and plain text format but you can also add your own using an intuitive template editor [see page 184].

By default, settings on the original message [see page 74] tab are defined to abort delivery of the original message. Also by default, auto response [see page 78] settings are set to send the automated response (i.e. the notification) message to the original sender and recipient(s) so that they know the message was stopped. All of these settings can be adjusted [see page 129] if required. For further information see adding an ethical walls policy on page 119.

Advanced

An advanced policy [see page 125] can be used to create a policy from first principles when your requirements do not match one of the predefined policy types above.

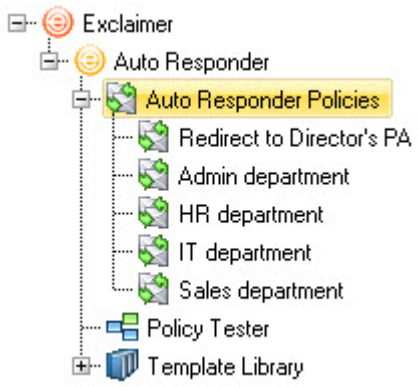
When an advanced policy is created, you can define basic information and conditions; once the policy is saved you can then edit it [see page 129] and update conditions [see page 84], exceptions [see page 91], original message [see page 74], auto response [see page 78], date range [see page 96] and next policy [see page 98] options to define more precise criteria and required actions to be taken when the policy is processed. For further information see adding an advanced policy on page 125.

Accessing Existing Policies

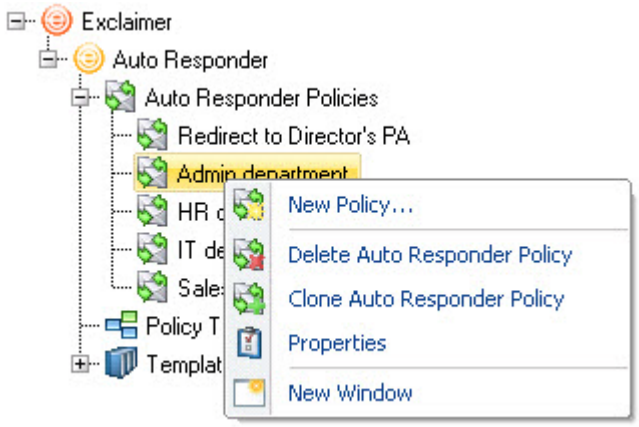
Within Exclaimer Auto Responder, policies are accessed via the Exclaimer console tree [see page 64], or using policy tabs [see page 66] from other branches of the console tree.

Navigating Policies Using the Console Tree

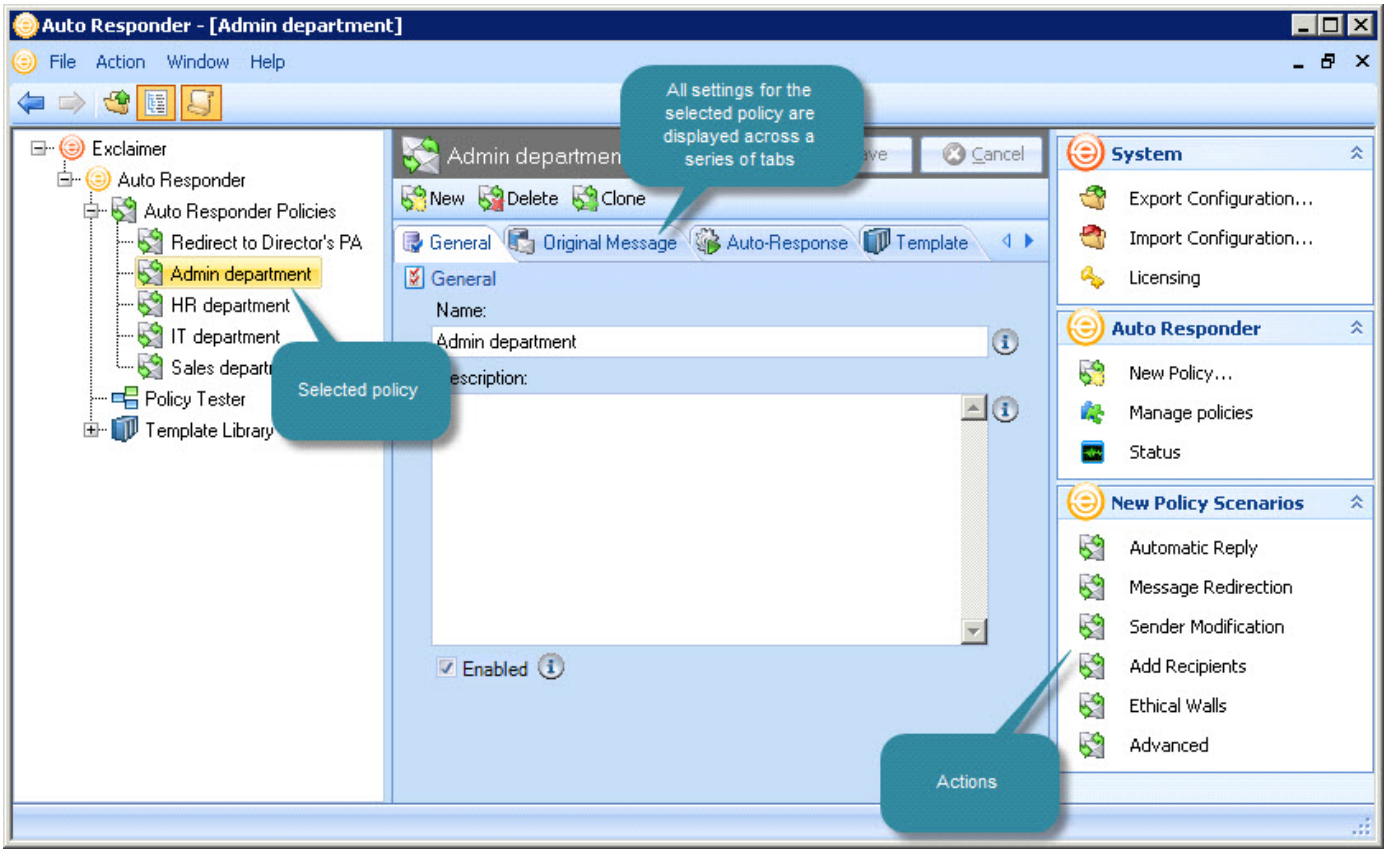
All work with policies is completed from the Auto Responder branch of the Exclaimer console tree [see page 20]:



From here you can view any existing policies (as child branches within the tree). Select any policy from the tree and right-click to view actions that can be taken with that policy:

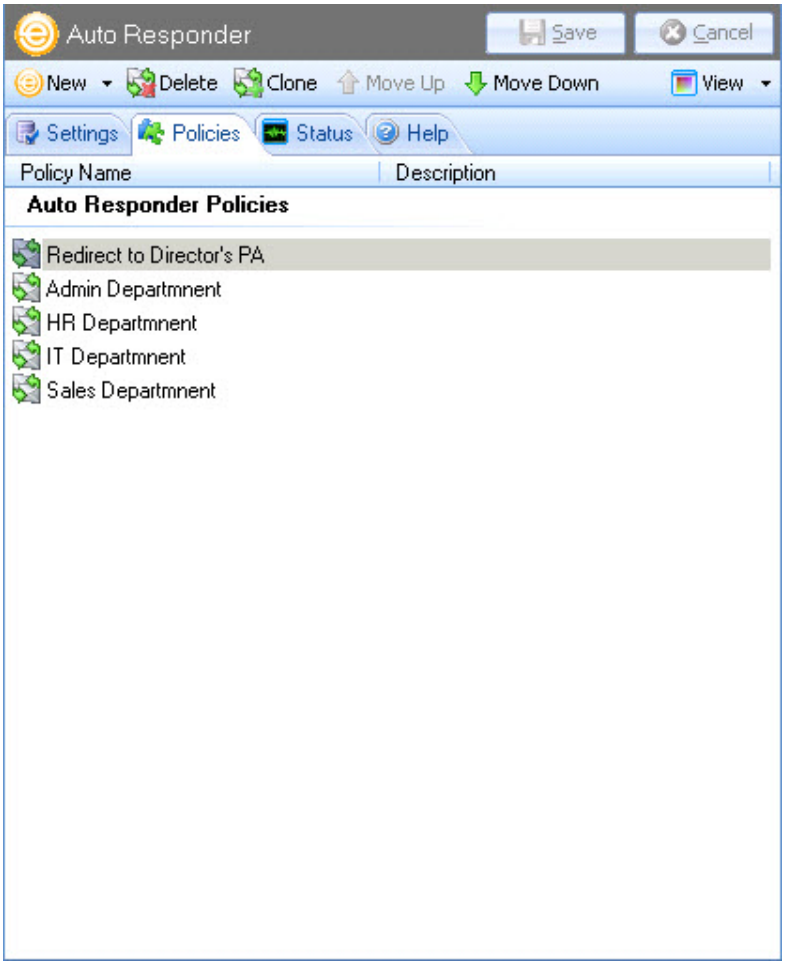


Having selected a policy from the tree, use the content pane to access all setup options and actions from the content pane:



Navigating Policies Using Policy Tabs

Existing policies can also be accessed from other branches of the console tree, via a policy tab in the content pane:

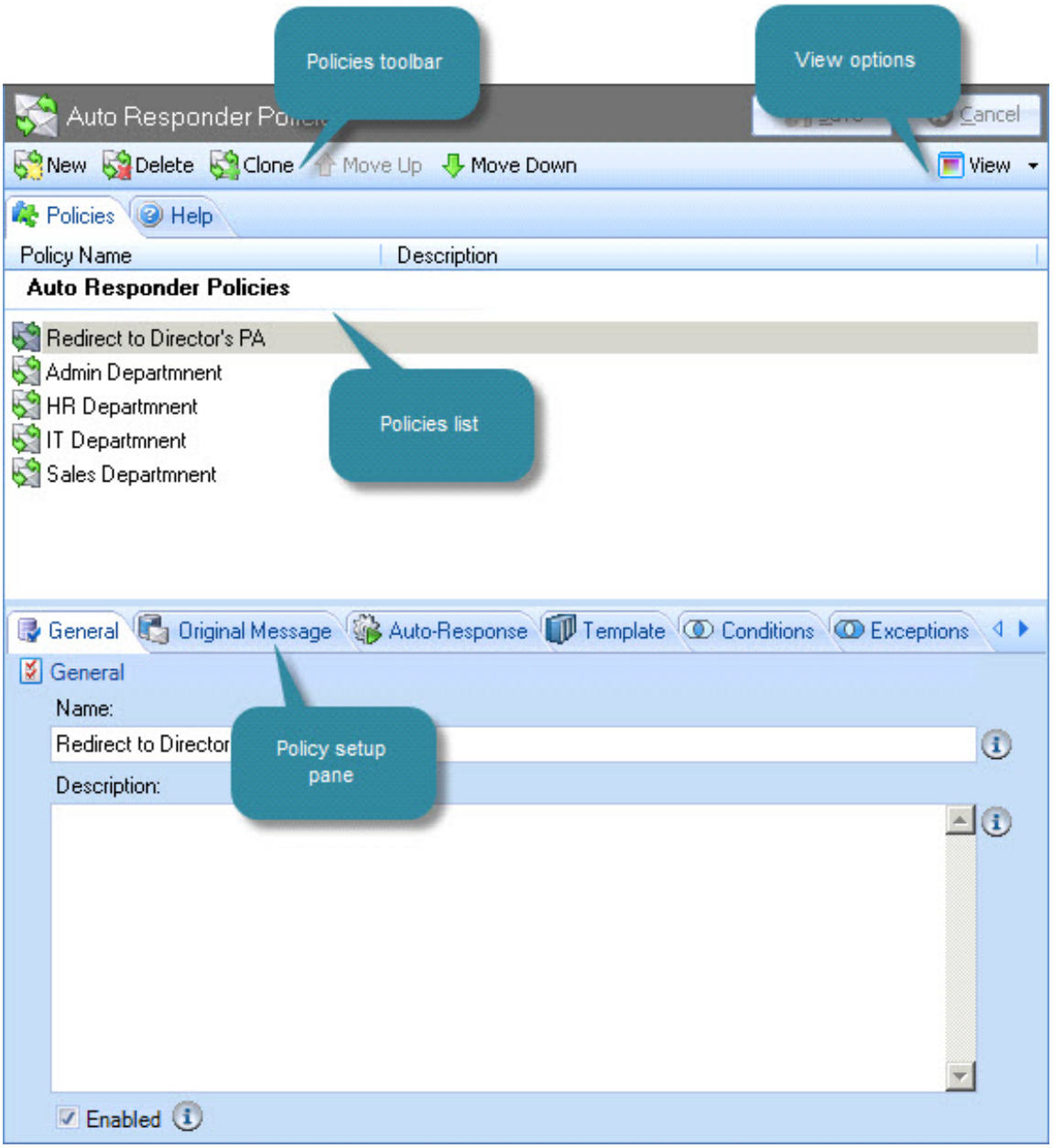


Policy tabs are available from the Auto Responder branch and also from the Auto Responder policies branch. The sequence in which policies are listed here is the same as the sequence shown in the console tree. **It is important to note that policies are processed in the order that they are listed here.**

You can use move up / move down options to change the sequence of this list, and use next policy [see page 98] options for greater control over processing sequence.

The Policies List

The policies tab contains quick access to existing policies. From here, you can select any policy from the list to view or edit its setup details:



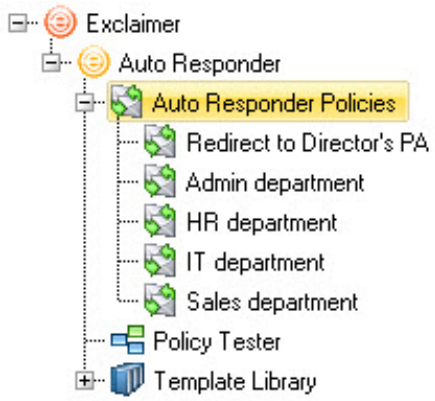
It is important to note that policies are processed in the order that they are listed here. You can use move up / move down [see page 50] options to change the sequence of this list, and use next policy [see page 98] options for greater control over processing sequence.

Available options are summarized in the following sections:

- The policy list [see page 68]
- The policy setup pane [see page 69]
- The policies toolbar [see page 69]
- View options [see page 70]
- Actions [see page 70]

The Policy List

All existing policies are listed in the upper section of the main content area; these are the same policies that you will see listed in the console tree:



It does not matter if you access policies from the console tree, or from the policy list shown here - use whichever method is most convenient for the task in hand.

The Policy Setup Pane

When a policy is selected in the policy list (the upper section of the content pane), all setup options for that policy are available in the lower section of the content pane. These options are organised across a series of tabs:

- General [see page 73]
- Template [see page 83]
- Original message [see page 74]
- Auto response [see page 78]
- Conditions [see page 84]
- Exceptions [see page 91]
- Date range [see page 96]
- Next policy [see page 98]

The Policies Toolbar

When the policies tab is displayed, the policies toolbar contains the following options:

Toolbar Option	Summary
New > Auto Responder policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy.
Delete	Select a policy from the list and use this option to remove [see page 130] it - the policy is removed from the list but is only permanently deleted when changes are saved [see page 38].
Clone	If you need to create a policy which is similar to an existing policy, use this option to clone [see page 128] (duplicate) the existing policy and then edit [see page 129] the duplicate version as required (this can be much quicker than creating a new policy from first principles).
Move Up / Move Down	Use these options to reorganize the policy list and determine the order in which policies are applied. Select a policy and click move up or move down as required.

View Options

The view option can be used to determine whether policies are displayed in list (details) form...

... or as large icons:

Actions

The following actions are available from the policies tab:

Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... section on page 39.
Import configuration...	Import a previously exported configuration file - see the import configuration... section on page 39.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.

Action	Select this option to...
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

The Anatomy of a Policy

An Auto Responder policy includes a range of settings which control how policies are processed and what (if any) auto responses are sent.

These settings are organized across a series of tabs, displayed in the content pane when a policy is selected:

- General [see page 73]
- Original message [see page 74]
- Auto response [see page 78]
- Template [see page 83]
- Conditions [see page 84]
- Exceptions [see page 91]
- Date range [see page 96]
- Next policy [see page 98]

The Anatomy of a Policy - General

Options on the general tab are used to define basic information for a policy. These settings determine how the policy is displayed throughout the system, and whether or not the policy is active:

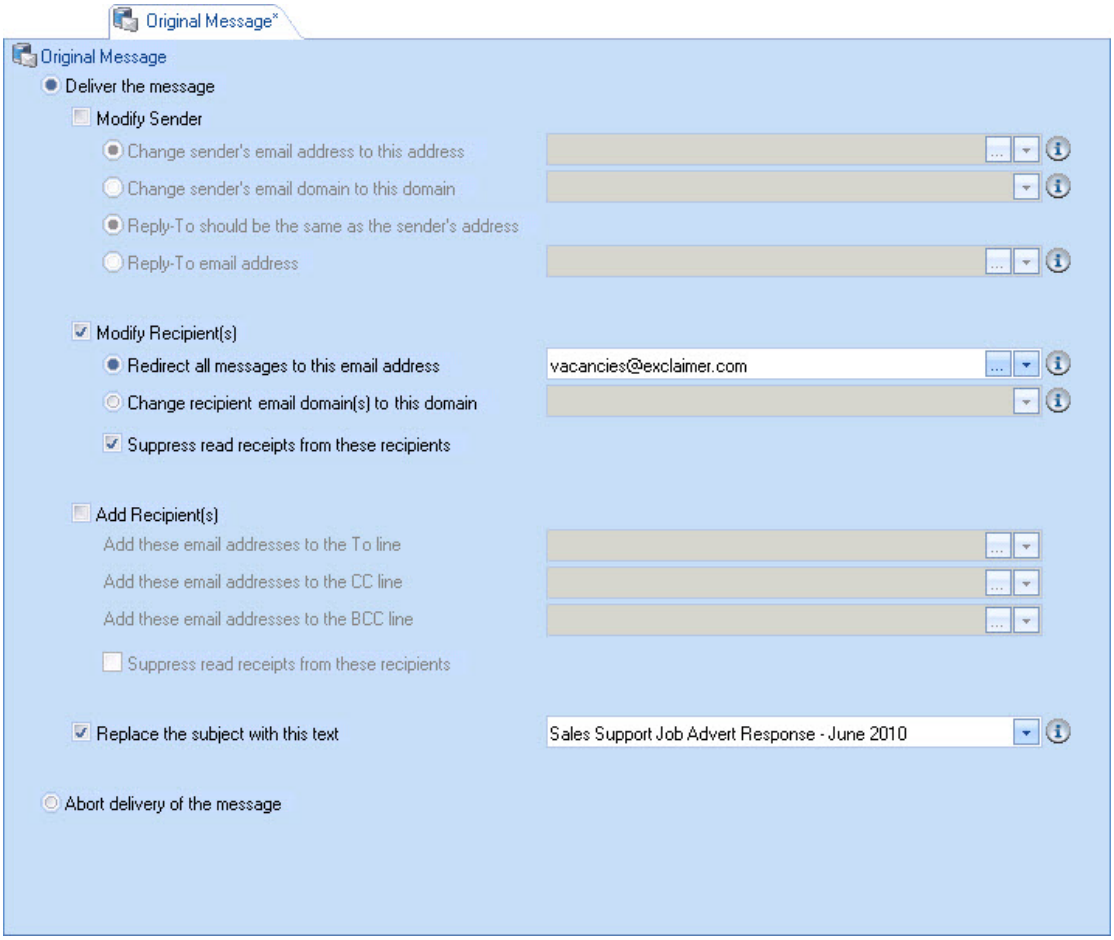
Options on this tab are summarized below:

Option	Summary
Name	Each policy must have a unique name. The name entered here is displayed in the Exclaimer console tree, and on any other policy lists.
Description	This field can be used to add any useful information for the policy - for example, usage notes, version history, background or explanatory information. The first line of description text is displayed in any policy lists [see page 66] (but not the console tree).
Enabled	Select this option to activate the policy. If a policy is not enabled, it will not run.

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

The Anatomy of a Policy - Original Message

Options on the original message tab are used to determine what action should be taken with the original email message when the policy is processed:



Options on this tab are summarized below:

Option	Summary
Deliver the message	Select this option to deliver the original email message when this policy is processed. If you are creating a simple automatic reply policy [see page 60], you would select this option and ignore further options on this page (remembering to define the required automated reply on the auto response [see page 78] tab). However, if you are creating a different policy type, it is likely that you will wish to specify modifications / actions for the original message using modify sender [see page 77] and/or modify recipient(s) [see page 77] and/or add recipient(s) [see page 77] and/or subject line [see page 77] options below.

Option	Summary
Modify Sender	Select this check box if you wish modify sender and/or reply-to details:

Modify sender option	Summary
Sender's email address	Replace the original sender's email address with the address specified here. You can: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email messages [see page 201] and message sender [see page 202] details are available for selection)
Sender's email domain	Replace the original sender's domain with the domain specified here. In this case, the local part of the email address would remain the same but the domain would be changed. For example, if you specify domain2.com here, an email address of joe.bloggs@domain1.com would be changed to joe.bloggs@domain2.com. You can: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email message [see page 201], message sender [see page 202], server [see page 224] and general [see page 224] details are available for selection).
Reply-to should be the same as the sender's address	Select this option if, when the message recipient selects the reply to option in Microsoft Outlook, the to address should be the same as the sender's email address.
Reply-to email address	Select this option if you wish to specify an alternative reply to email address. When the message recipient selects the reply to option in Microsoft Outlook, the to address will be the address specified here rather than the sender's email address. You can: ▪ Type the required value directly into the field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see

Option	Summary
	page 198] from a drop-down list (any fields that are associated with email message [see page 201] and message sender [see page 202] details are available for selection)
Modify recipient(s)	Select this check box if you wish modify recipient details for the message:

Modify sender option	Summary
Redirect all messages to this email address	Ignore any recipients defined in the original message and redirect the message to the addressee(s) specified here. You can: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email message [see page 201] and message sender [see page 202] details are available for selection)
Change recipient domain(s) to this domain	Replace the recipient's domain with the domain specified here. In this case, the local part of the email address would remain the same but the domain would be changed. For example, if you specify domain2.com here, an email address of joe.bloggs@domain1.com would be changed to joe.bloggs@domain2.com. You can: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email messages [see page 201], message sender [see page 202], server [see page 224] and general [see page 224] details are available for selection).
Suppress read receipts from these recipients	Select this option if you wish to prevent read receipts being generated from modified recipients.

Option	Summary
Add recipient(s)	Select this check box if you wish keep any recipients specified in the original message but add further recipients:

Modify sender option	Summary
Add these addresses to the To line	Specify email addresses to be added as recipients of the original email message.
Add these addresses to the CC line	Specify email addresses to be copied in on the original email message.
Add these addresses to the BCC line	Specify email addresses to be blind copied in on the original email message.
Suppress read receipts from these recipients	Select this option if you wish to prevent read receipts being generated from added recipients.

These options are most commonly used in add recipients policies [see page 62]. When choosing to add addresses you can:

- Type the required value directly into the associated field
- Use the browse button to browse user accounts and domains

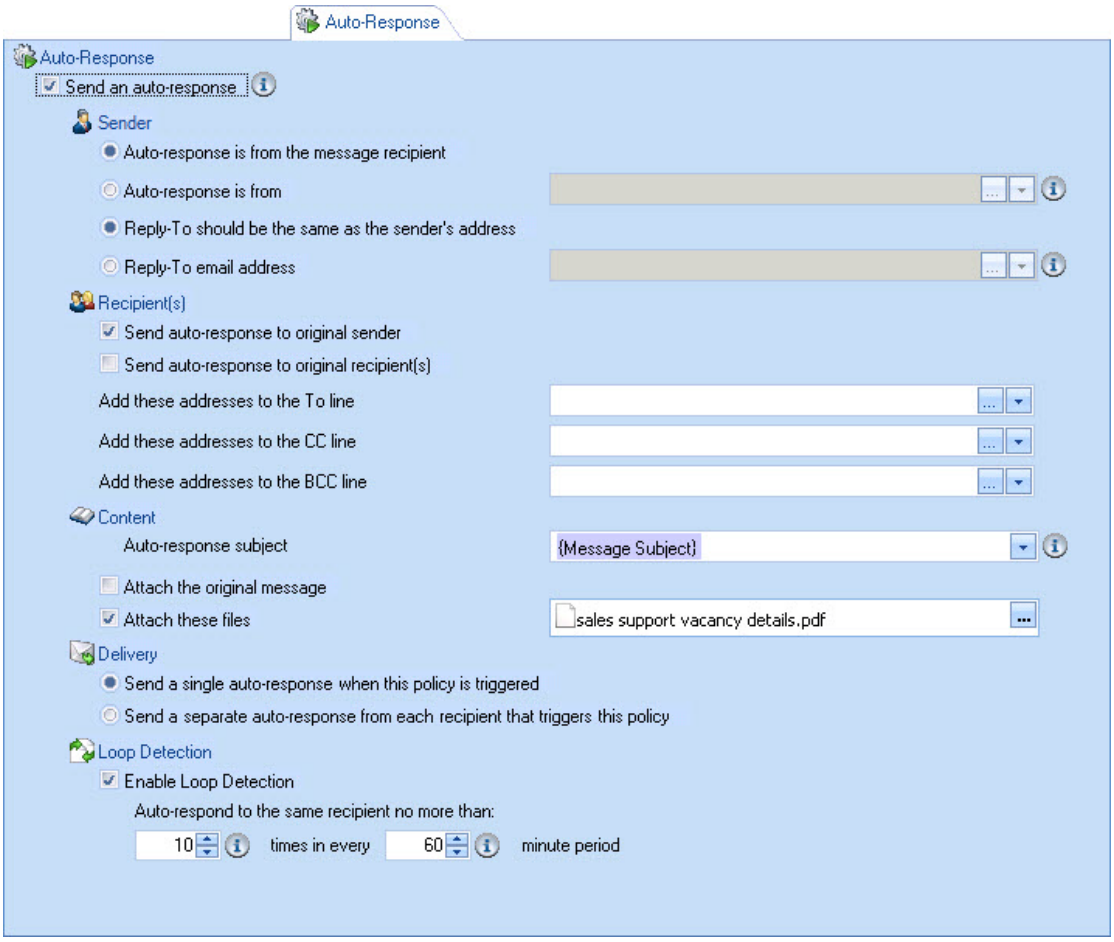
Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email message [see page 201] and message sender [see page 202] details are available for selection).

Replace the subject with this text	Select this option and type required text to replace the subject line of the original email message. Alternatively, use the drop-down list of fields [see page 198] to dynamically insert text from an Active Directory field.
Abort delivery of the message	Select this option to abort transmission of the original email message. This option is most commonly used in ethical walls policies [see page 62].

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

The Anatomy of a Policy - Auto Response

Options on the auto response tab are used to determine whether an automated response is sent when this policy is processed and if so, how that response should be handled:



Options on this tab are summarized below:

Option	Summary
Send an auto response	Select this option to send an automated response when this policy is processed. If this option is not selected, an automated response will not be sent. Having selected this option, check sender [see page 80], recipient(s) [see page 80], content [see page 81] and loop detection [see page 82] options to define how the response is sent.

Option	Summary
Sender	Use these options to control sender and reply-to details for the automated response message. You can select one from and one reply-to option:

Modify sender option	Summary
Auto response is from the message recipient	Select this option for the message recipient to be shown in the from field of the automated response message.
Auto response is from	If you wish the automated response to be from someone other than the message recipient, select this option and then: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email message [see page 201], message recipient [see page 209] and message sender [see page 202] details are available for selection)
Reply-to should be the same as the sender's address	Select this option if, when the message recipient selects the reply to option in Microsoft Outlook, the to address should be the same as the sender's email address.
Reply-to email address	Select this option if you wish to specify an alternative reply to email address. When the message recipient selects the reply to option in Microsoft Outlook, the to address will be the address specified here rather than the sender's email address. You can: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email message [see page 201], message recipient [see page 209] and message sender [see page 202] details are available for selection)

Option	Summary
Recipient(s)	Use these options to control who the automated response message is sent to. You can select one or more of the following options: **Modify sender option** / **Summary** Send auto response to original sender — Select this option to send an automated response to the person who sent the original message. Send auto response to original recipient(s) — Select this option to send an automated response to all original recipients. Add these addresses to the To line — Specify email addresses to be added as recipients of the automated response message. Add these addresses to the CC line — Specify email addresses to be copied in on the automated response message. Add these addresses to the BCC line — Specify email addresses to be blind copied in on the automated response message. When choosing to add addresses you can: ▪ Type the required value directly into the associated field ▪ Use the browse button to browse user accounts and domains ▪ Use the arrow to select an Active Directory field [see page 198] from a drop-down list (any fields that are associated with email message [see page 201], message recipient [see page 209] and message sender [see page 202] details are available for selection)

Option	Summary
Content	Use these options to control how the content of an automated response message should be handled:

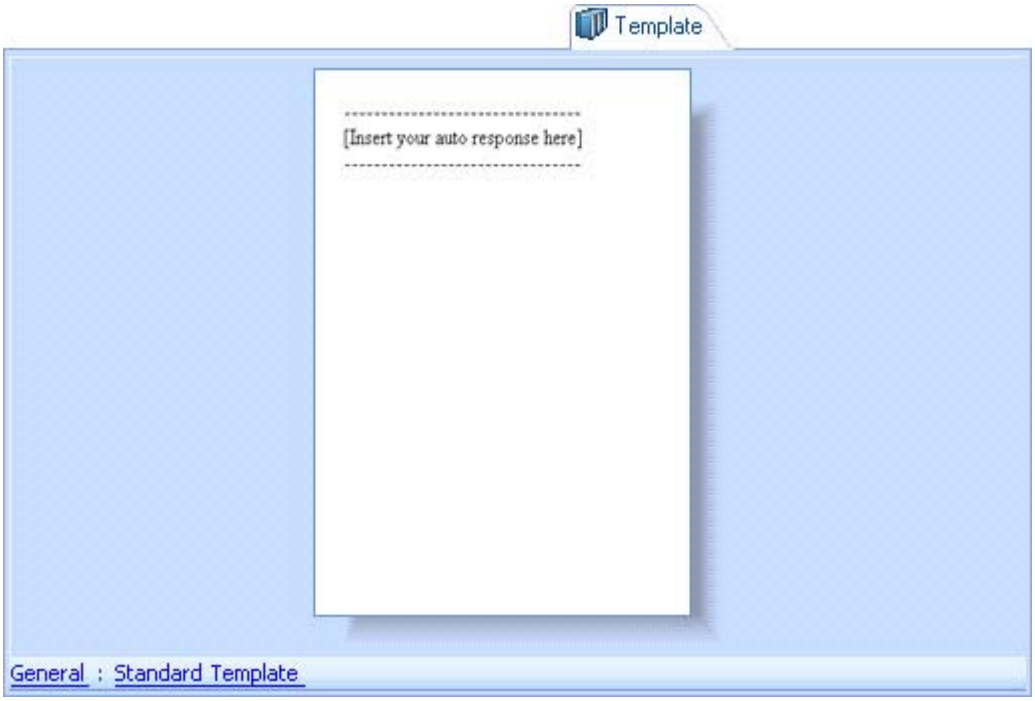
Modify sender option	Summary
Auto response subject	Specify required subject line for the automated response message. By default this is set to a message subject field which means that the original message subject will be used. You can change this if required - for example you might choose to type 'RE:' in front of the field so the subject line of the automated response message will show 'RE:' followed by the original message subject line. You can enter any static text and/or use the arrow to select other fields [see page 198] from a drop-down list (any fields that are associated with email message [see page 201], recipient [see page 209], sender [see page 202], dynamic content [see page 215], server [see page 224] and general [see page 224] details are available for selection). For example, you might define a subject line which reads 'Re. your message sent to Joe Bloggs' where Joe Bloggs is dynamically replaced with the original message recipient name. To achieve this, you would type: Re. your message sent to and then insert the message recipients field: Your message to {Message Recipients}
Attach the original message	Select this option if you wish to send a copy of the original email message as an attachment with the automated response. For further information about including the original message in automated responses, see how do I include the original message in an automatic reply? on page 231.
Attach these files	Select this option if you wish to attach selected files to the automated response message (for example, if you are responding to job applications you might wish to attach company literature). Use the browse button to navigate local and network drives to select required attachments. For further information see how can I send file attachments with an automatic reply? on page 149.
Send a single auto response when this policy is triggered	If an original message is addressed to multiple recipients, select this option if you wish to send just one automated response.
Send a separate auto response from each recipient that triggers this policy	If an original message is addressed to multiple recipients, select this option if you wish to send an automated response for each individual recipient (thus the original message sender will receive multiple automated responses).

Option	Summary
Loop Detection	The purpose of this feature is to ensure that Auto Responder does not respond to auto responders (of any software type) so many times that it compromises your mail server. Enter the number of times that an automated response can be made in the specified time period.

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

The Anatomy of a Policy - Template

The template tab shows which template is associated with the selected policy:



The associated template for an automated response is previewed in the content pane. Here, a sample email is used to show how any content, layout and formatting in the template will be applied to messages. From here you can:

- Double click anywhere in the content pane to edit the template in the template editor [see page 184]
- Use the breadcrumb trail at the bottom of the window to open the template library [see page 164]

Changes are retained if you move to other tabs within the content pane. When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes across all tabs. Alternatively, use the cancel button to abandon all changes.

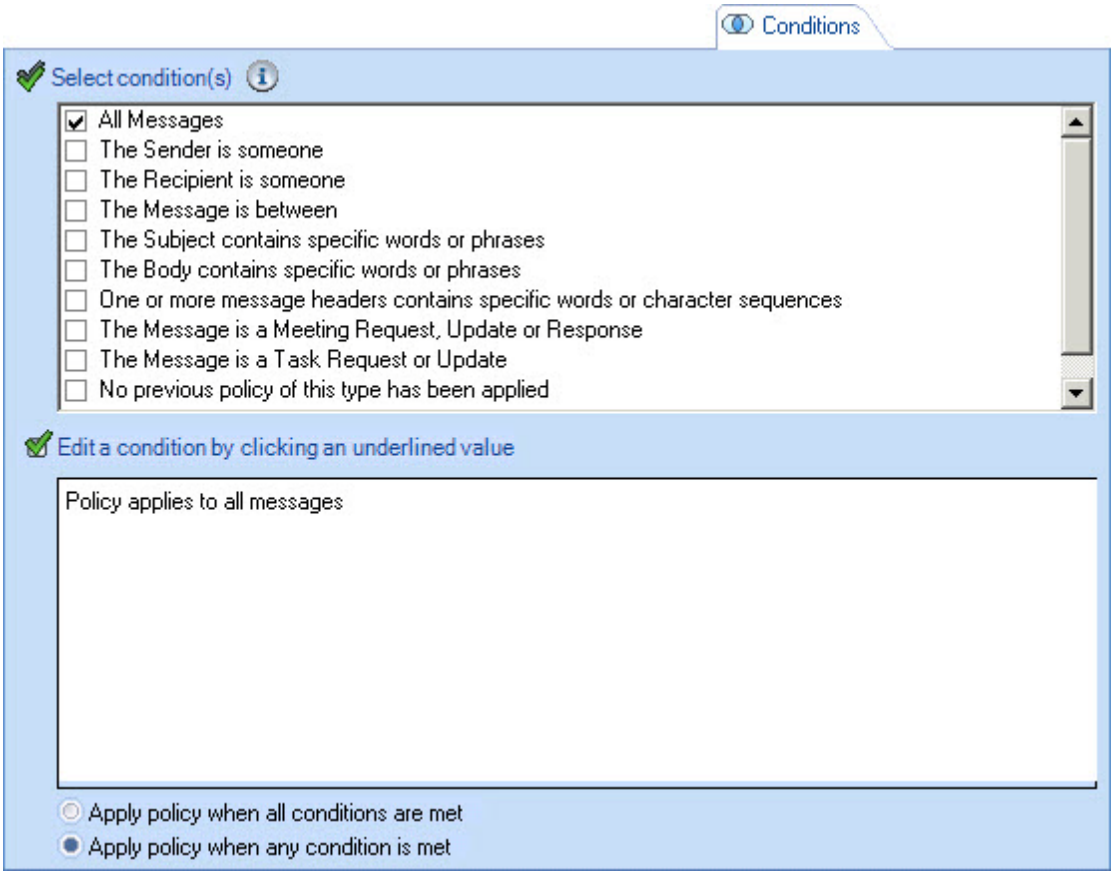
The Template Breadcrumb Trail

At the bottom of the template preview, a breadcrumb trail displays the name of the template being used, together with its parent category [see page 169] in the template gallery.

Click an entry in the breadcrumb trail to open the template library [see page 164] to view / select templates.

The Anatomy of a Policy - Conditions

The conditions tab is used to set criteria [see page 85] which determines the circumstances under which a policy is applied:



Once a condition is selected, any options [see page 85] for that condition are displayed as hyperlinks in the lower pane - select these links to refine the condition. For instance, selecting the someone link displays further options to refine the sender is someone condition.

Each time a selection is made, confirmation of the selection and any further options [see page 85] are displayed in the lower pane.

At least one condition must be set to apply a policy. If a condition is not selected, the default condition of all messages is used. See the options summary on page 85 for a summary of available conditions.

Available Options for Setting Conditions

When working with conditions [see page 84] for a policy, the following options are available:

- [x] All Messages
- [ ] The Sender is someone
- [ ] The Recipient is someone
- [ ] The Message is between
- [ ] The Subject contains specific words or phrases
- [ ] The Body contains specific words or phrases
- [ ] One or more message headers contains specific words or character sequences
- [ ] The Message is a Meeting Request, Update or Response
- [ ] The Message is a Task Request or Update
- [ ] No previous policy of this type has been applied
- [ ] The message is signed or encrypted

When a condition is selected, further options are available, as summarized below:

- All messages [see page 86]
- The Sender is someone [see page 86]
- The Sender is a specific user [see page 86]
- The Sender is a member of an Active Directory group [see page 86]
- The Sender is a member of an Active Directory domain or organizational unit [see page 86]
- The Sender has one or more specific Active Directory attributes [see page 86]
- The Sender address contains specific character sequences [see page 86]
- The Sender is inside or outside the organization [see page 86]
- The Sender is an Active Directory contact [see page 86]
- The Recipient is someone [see page 87]
- The Recipient is a specific user or distribution group [see page 87]
- The Recipient is a member of an Active Directory group [see page 87]
- The Recipient is a member of an Active Directory domain or organizational unit [see page 87]
- The Recipient has one or more specific Active Directory attributes [see page 87]
- The Recipient address contains specific character sequences [see page 87]
- The Recipient is inside or outside the organization [see page 87]
- The Recipient is an Active Directory contact [see page 87]
- The Recipient is in the To or Cc field of the message [see page 87]
- The message is between [see page 87]
- The Subject contains specific words or phrases [see page 88]
- The Body contains specific words or phrases [see page 88]

- One or more message headers contains specific words or character sequences [see page 88]
- The Message is a Meeting Request, Update or Response [see page 88]
- The Message is a Task Request or Update [see page 88]
- No previous policy of this type has been applied [see page 88]
- The message is signed or encrypted [see page 88]

All Messages

This is a blanket or 'wildcard' condition which will apply the policy to all messages.

The Sender is Someone

When selected, a someone link is displayed in the lower pane; use this link to access further options, as summarized in the following sections.

The Sender is a Specific User

Use the list of users link to browse and select a user from the user list.

The Sender is a Member of an Active Directory Group

Use the Active Directory group link to browse and select the required group from a list of Active Directory groups.

The Sender is a Member of an Active Directory Domain or Organizational Unit

Use the domain or organizational unit link to browse and select the required domain or unit from a container list..

The Sender has One or More Specific Active Directory Attributes

Use the Active Directory attribute values link to open the configure attributes window [see page 89] to define queries to be resolved for matching.

The Sender Address Contains Specific Character Sequences

Use the character sequences link to define character sequences to be matched in the sender's email address.

The Sender is Inside or Outside the Organization

Use the inside link to match messages where the sender is either internal or external to the organization.

The Sender is an Active Directory Contact

Use is / is not links to specify whether external addresses which have (or do not have) an AD contact will trigger the policy.

The Recipient is Someone

When selected, a someone link is displayed in the lower pane; use this link to access further options, as summarized in the following sections.

The Recipient is a Specific User or Distribution Group

Use the list of users or distribution lists link to browse and select a user or distribution list from the user list.

The Recipient is a Member of an Active Directory Group

Use the Active Directory group link to browse and select the required group from a list of Active Directory groups.

The Recipient is a Member of an Active Directory Domain or Organizational Unit

Use the domain or organizational unit link to browse and select the required domain or unit from a container list.

The Recipient Has One or More Specific Active Directory Attributes

Use the Active Directory attribute values link to open the configure attributes window [see page 89] to define queries to be resolved for matching.

The Recipient Address Contains Specific Character Sequences

Use the character sequences link to define character sequences to be matched in the sender's email address.

The Recipient is Inside or Outside The Organization

Use the inside link to match messages where the recipient is either internal or external to the organization.

The Recipient is an Active Directory Contact

Use is / is not links to specify whether external addresses which have (or do not have) an AD contact will trigger the policy.

The Recipient is in the To or Cc Field of the Message

Use the to or cc field to match messages where the recipient is in the To or the Cc field of the email, or where the recipient is only in the to field, or where the recipient is only in the cc field.

The Message is Between

Use the A and B links to specify two parties between which email communication may or may not take place. This condition is commonly used when defining ethical walls [see page 62] policies.

The Subject Contains Specific Words or Phrases

Use the words or phrases link to specify given words or phrases to be matched in the message subject line. Use the words or phrases window to enter required items to be matched. If a single entry contains multiple words, it is considered to be a phrase. Use check boxes at the bottom of the window to choose whether matching should take place if any or all words/phrases are matched, and whether matching is case sensitive.

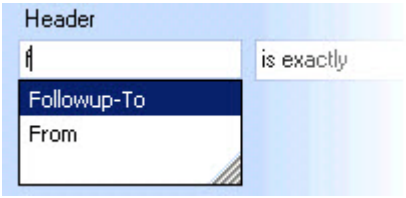
The Body Contains Specific Words or Phrases

Use the words or phrases link to specify given words or phrases to be matched in the message body. Use the words or phrases window, as described above.

One or More Message Headers Contains Specific Words or Character Sequences

Match messages based on message header fields. Use message headers and words or character sequences links to enter header fields and values to be matched.

The header field uses intellisense for common message header fields, therefore it suggests an entry based on what you type. For example, if you type the letter 'T' into this field, the header 'To' is suggested, whereas if you type 'f' into the field, the Followup-To' and 'From' headers are suggested:



The Message is a Meeting Request, Update or Response

Match messages if they are a meeting request, an updated meeting request, or a response to a meeting request.

The Message is a Task Request or Update

Match messages if they are a task request or an update to a task request.

No previous policy of this type has been applied

Use this as a 'catch all' condition. This is commonly used as the condition for a final policy in a policy chain [see page 98].

The Message is Signed or Encrypted

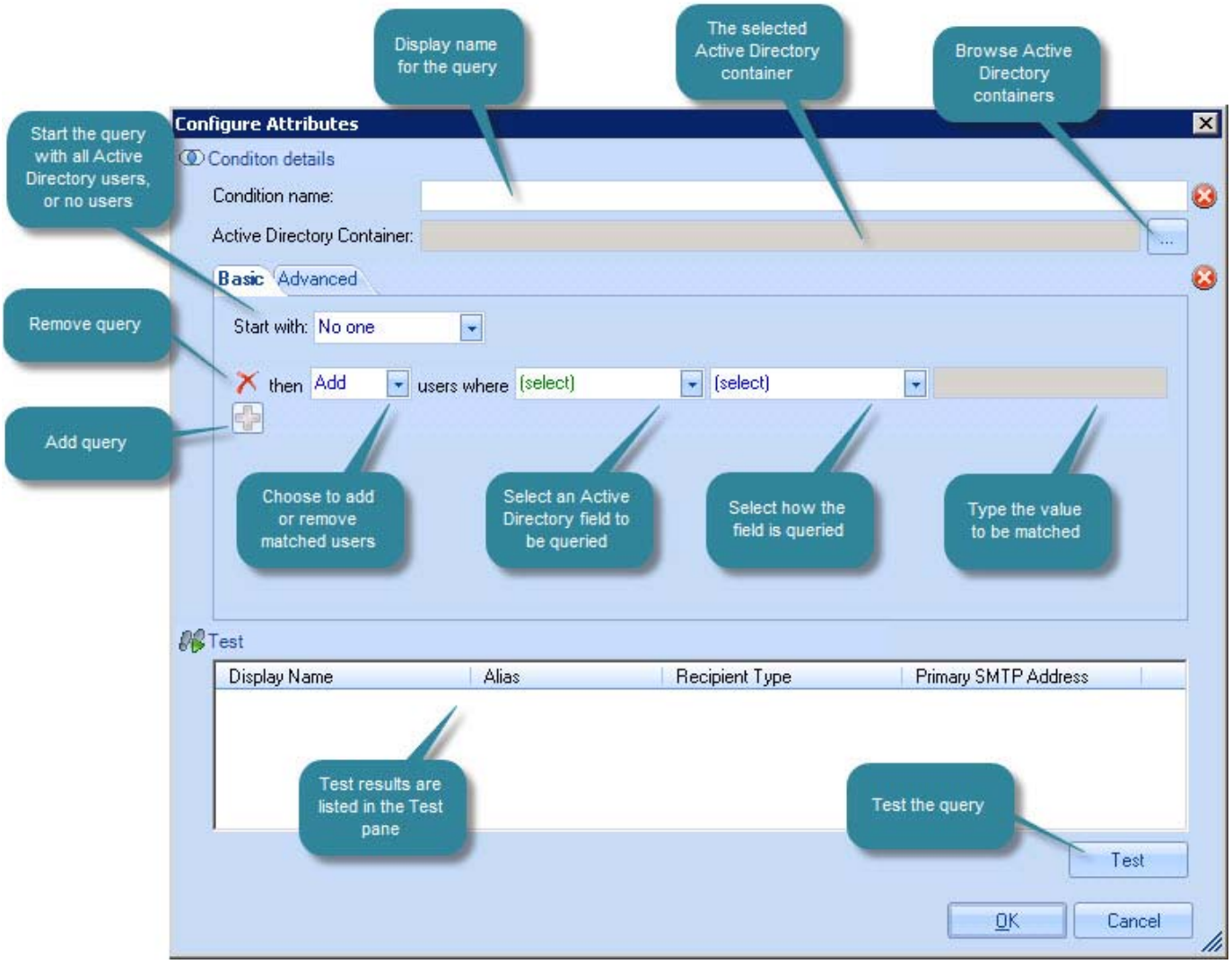
Use this condition to set criteria based upon whether messages are signed or encrypted. Use the encrypted link to open selection options and switch to signed, or use the signed link to open selection options and switch to encrypted.

> At least one condition must be set when a policy is defined. If a condition is not selected, the default condition of **all messages** is used.

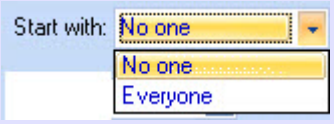
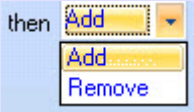
Creating Queries With the Configure Attributes Window

The configure attributes window allows you to define conditions [see page 84] and exceptions [see page 91] based on queries that are run on Active Directory user attributes - for example, you might want to define a policy to match all users within a given department, or a specific country, or with a certain manager.

With Exclaimer Auto Responder, you can define queries based on the full range of Active Directory attributes. The configure attributes window is opened when defining a condition [see page 84] or an exception [see page 91] using the sender/recipient is someone and then the sender/recipient has one or more specific Active Directory attributes options:



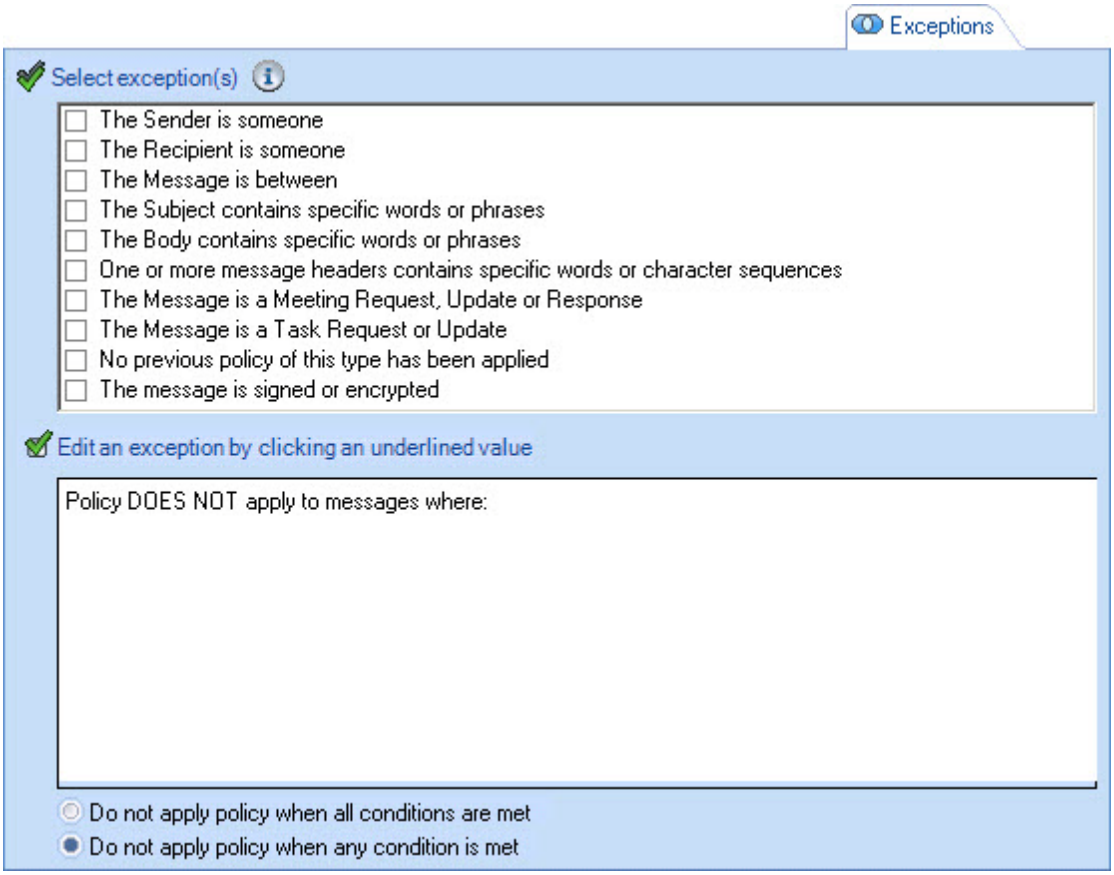
Available options shown here are summarized below:

Field	Summary
Condition name	Enter a name for this query. This name is displayed in the main condition/exception window: It is advisable to specify a name that summarizes the purpose of the query. If you have multiple administrators, you might also choose to add version change dates here.
Active Directory container	Use the browse button to select an Active Directory container, or leave blank to search the entire Active Directory.
Start with	Choose to start the query with no one (so the query will start with nothing and add matched users) or everyone (so the query will start with all Active Directory users and remove matched users): 
	Use this icon to remove a query line.
	Use this icon to add a new query line.
then...	Choose to add or remove matched users:  Defaults to add if you have chosen to start with no one and remove if you have chosen to start with everyone).
users where...	Select the Active Directory field to be queried, then how it should be queried (equal to, does not equal, starts with, ends with, etc) and finally enter a value to be matched against.
Test	Use the test option to run the query and view matched users in the test pane.

See how do I create a policy based on specific Active Directory attributes? on page 135 for a working example of a policy based on an attribute query.

The Anatomy of a Policy - Exceptions

Exceptions are used to specify any exceptions to conditions [see page 84] which have been set. For example, if you have defined a condition to match everyone within a given department, you might define an exception to exclude individual people within that department. Use the exceptions tab to set required criteria [see page 92]:



Once an exception is selected, any options [see page 92] for that exception are displayed as hyperlinks in the lower pane - select these links to refine the exception. For instance, selecting the someone link in the example above displays further options to refine the sender is someone exception.

Each time a selection is made, confirmation of the selection and any further options [see page 92] are displayed in the lower pane.

See the exceptions - options summary on page 92 for a working example of a policy based on an attribute query.

Available Options for Setting Exceptions

When working with exceptions [see page 91] for a policy, the following options are available:

- ☐ The Sender is someone
- ☐ The Recipient is someone
- ☐ The Message is between
- ☐ The Subject contains specific words or phrases
- ☐ The Body contains specific words or phrases
- ☐ One or more message headers contains specific words or character sequences
- ☐ The Message is a Meeting Request, Update or Response
- ☐ The Message is a Task Request or Update
- ☐ No previous policy of this type has been applied
- ☐ The message is signed or encrypted

When an exception is selected, further options are available, as summarized below:

- The Sender is someone [see page 93]
- The Sender is a specific user [see page 93]
- The Sender is a member of an Active Directory group [see page 93]
- The Sender is a member of an Active Directory domain or organizational unit [see page 93]
- The Sender has one or more specific Active Directory attributes [see page 93]
- The Sender address contains specific character sequences [see page 93]
- The Sender is inside or outside the organization [see page 93]
- The Sender is an Active Directory contact [see page 93]
- The Recipient is someone [see page 93]
- The Recipient is a specific user or distribution group [see page 93]
- The Recipient is a member of an Active Directory group [see page 94]
- The Recipient is a member of an Active Directory domain or organizational unit [see page 94]
- The Recipient has one or more specific Active Directory attributes [see page 94]
- The Recipient address contains specific character sequences [see page 94]
- The Recipient is inside or outside the organization [see page 94]
- The Recipient is an Active Directory contact [see page 94]
- The Recipient is in the To or Cc field of the message [see page 94]
- The message is between [see page 94]
- The Subject contains specific words or phrases [see page 94]
- The Body contains specific words or phrases [see page 94]
- One or more message headers contains specific words or character sequences [see page 95]
- The Message is a Meeting Request, Update or Response [see page 95]

- The Message is a Task Request or Update [see page 95]
- No previous policy of this type has been applied [see page 95]
- The message is signed or encrypted [see page 95]

The Sender is Someone

When selected, a someone link is displayed in the lower pane; use this link to access further options, as summarized in the following sections.

The Sender is a Specific User

Use the list of users link to browse and select a user from the user list.

The Sender is a Member of an Active Directory Group

Use the Active Directory group link to browse and select the required group from a list of Active Directory groups.

The Sender is a Member of an Active Directory Domain or Organizational Unit

Use the domain or organizational unit link to browse and select the required domain or unit from a container list.

The Sender Has One or More Specific Active Directory Attributes

Use the Active Directory attribute values link to open the configure attributes window [see page 89] to define queries to be resolved for matching.

The Sender Address Contains Specific Character Sequences

Use the character sequences link to define character sequences to be matched in the sender's email address.

The Sender is Inside or Outside the Organization

Use the inside link to match messages where the sender is either internal or external to the organization.

The Sender is an Active Directory Contact

Use the is / is not link to specify whether external addresses which have (or do not have) an AD contact will trigger the policy.

The Recipient is Someone

When selected, a someone link is displayed in the lower pane; use this link to access further options, as summarized in the following sections.

The Recipient is a Specific User or Distribution Group

Use the list of users or distribution lists link to browse and select a user or distribution list from the user list.

The Recipient is a Member of an Active Directory Group

Use the Active Directory group link to browse and select the required group from a list of Active Directory groups.

The Recipient is a Member of an Active Directory Domain or Organizational Unit

Use the domain or organizational unit link to browse and select the required domain or unit from a container list.

The Recipient Has One or More Specific Active Directory Attributes

Use the Active Directory attribute values link to open the configure attributes window [see page 89] to define queries to be resolved for matching.

The Recipient Address Contains Specific Character Sequences

Use the character sequences link to define character sequences to be matched in the sender's email address.

The Recipient Is Inside or Outside The Organization

Use the inside link to match messages where the recipient is either internal or external to the organization.

The Recipient is an Active Directory Contact

Use is / is not links to specify whether external addresses which have (or do not have) an AD contact will trigger the policy.

The Recipient is in the To or Cc Field of The Message

Use to or cc fields to match messages where the recipient is in the to or the cc field of the email, or where the recipient is only in the to field, or where the recipient is only in the cc field.

The message is Between

Use the A and B links to specify two parties between which email communication may or may not take place. This condition is commonly used when defining ethical walls [see page 62] policies.

The Subject Contains Specific Words or Phrases

Use the words or phrases link to specify given words or phrases to be matched in the message subject line. Use the words or phrases window to enter required items to be matched. If a single entry contains multiple words, it is considered to be a phrase. Use check boxes at the bottom of the window to choose whether matching should take place if any or all words/phrases are matched, and whether matching is case sensitive.

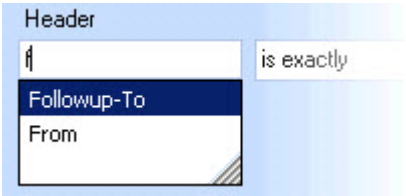
The Body Contains Specific Words or Phrases

Use the words or phrases link to specify given words or phrases to be matched in the message body. Use the words or phrases window, as described above.

One or More Message Headers Contains Specific Words or Character Sequences

Match messages based on message header fields. Use message headers and words or character sequences links to enter header fields and values to be matched.

The header field uses intellisense for common message header fields, therefore it suggests an entry based on what you type. For example, if you type the letter 'T' into this field, the header 'To' is suggested, whereas if you type 'f' into the field, the 'Followup-To' and 'From' headers are suggested:



The Message is a Meeting Request, Update or Response

Match messages if they are a meeting request, an updated meeting request, or a response to a meeting request.

The Message is a Task Request or Update

Match messages if they are a task request or an update to a task request.

No Previous Policy of This Type Has Been Applied

Use this as a 'catch all' condition. This is commonly used as the condition for a final policy in a policy chain [see page 98].

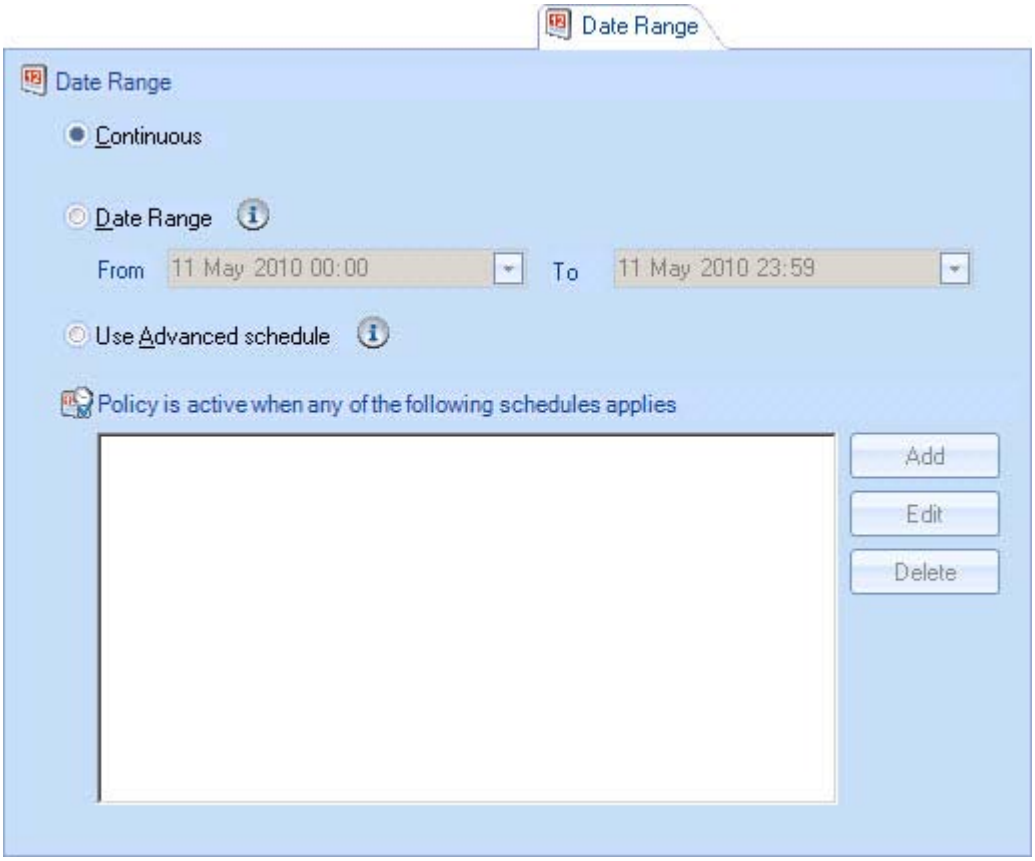
The Message is Signed or Encrypted

Use this condition to set criteria based upon whether messages are signed or encrypted. Use the encrypted link to open selection options and switch to signed, or use the signed link to open selection options and switch to encrypted.

> At least one condition must be set to apply policies. If a condition is not selected, the default condition of **all messages** is used.

The Anatomy of a Policy - Date Range

Options on the date range tab are used to set any date / time limitations for a policy:

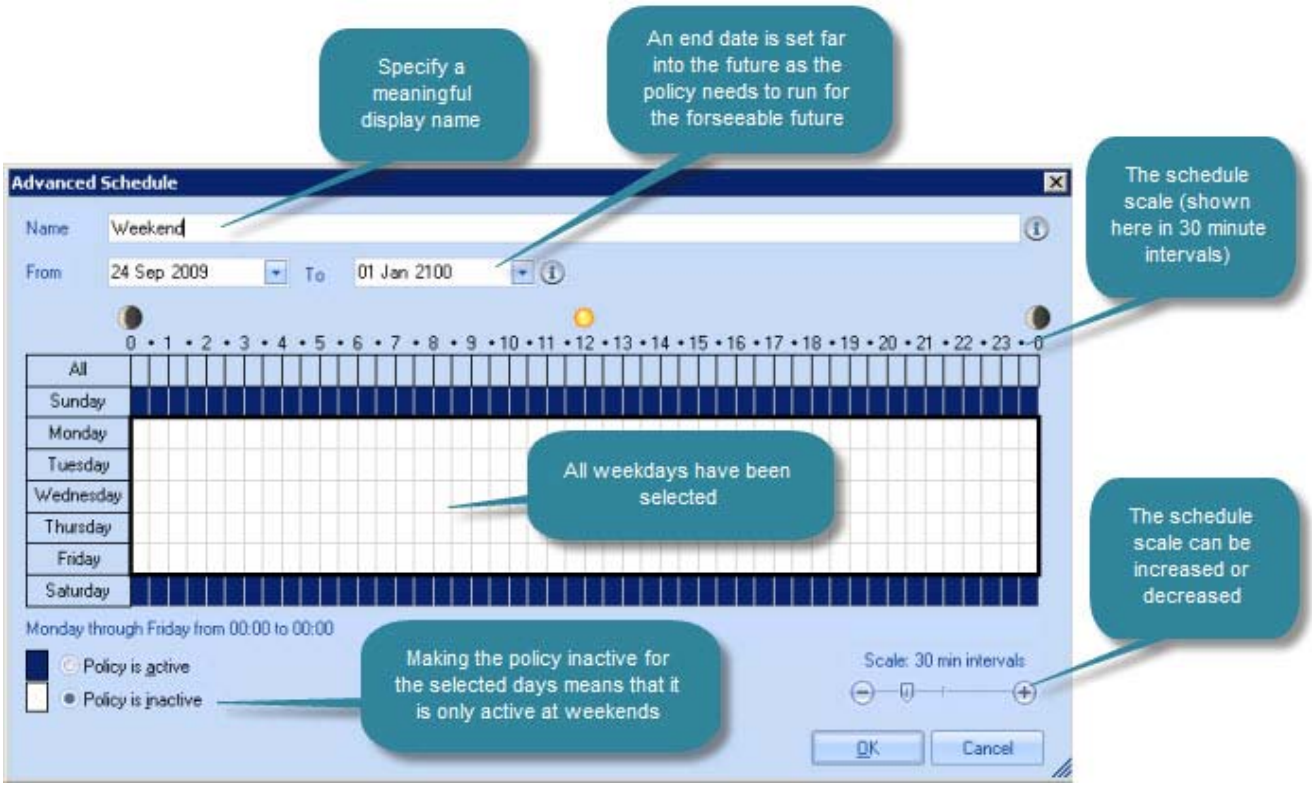


By default, the date range tab is set to continuous, which means that there are no date or time restrictions associated with the policy. Alternatively, specific to and from dates can be set so that the policy has a start/end time, or a detailed schedule can be set.

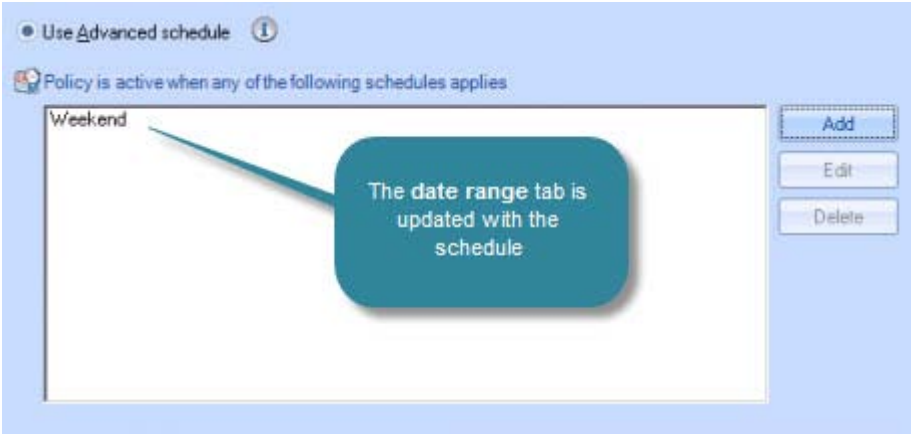
Using the Advanced Schedule

The advanced schedule works by selecting days of the week that the policy is active or inactive. Each day is split into time intervals, which can be adjusted using a sliding scale at the bottom of the window; this means that policies can be set to run on precise days at precise times.

To use the advanced schedule, click the use advanced schedule radio button and then click add. The example below shows how the schedule is used to create a policy that is only active at weekends:



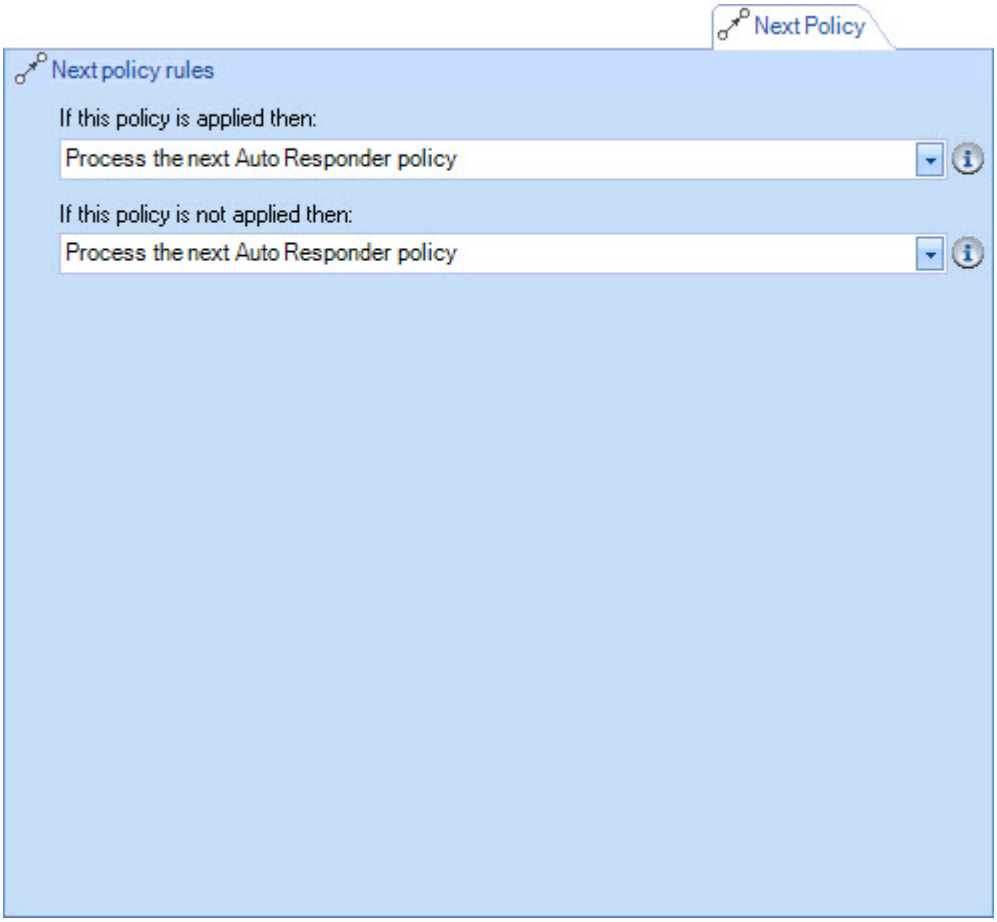
Having made required date and time selections, click OK to exit back to the updated date range tab:



To update an existing schedule, select its name and click edit. Similarly, click delete to remove the selected schedule.

The Anatomy of a Policy - Next Policy

If you have a number of policies which are dependent upon each other, you can create a 'policy chain' using the next policy tab:



Whilst you control the sequence in which policies are processed using the policy tab [see page 67], the next policy tab allows you to define specific policy chains based on whether the previous policy in the chain is or is not applied. These options are:

If this policy is applied then:

- Process the next Auto Responder policy
- Don't process anymore Auto Responder policies

If this policy is not applied then:

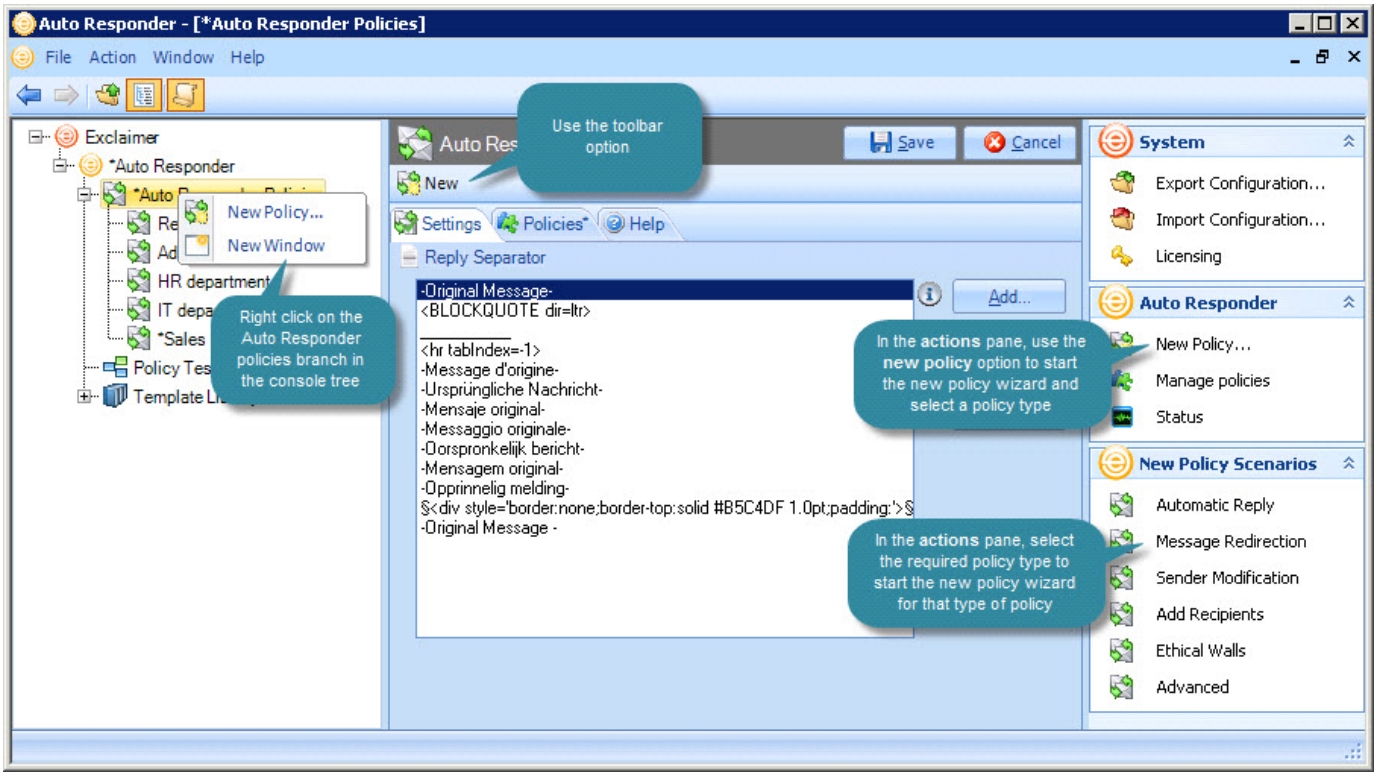
- Process the next Auto Responder policy
- Don't process anymore Auto Responder policies

You can use these options for a wide range of scenarios, creating policy chains as simple or as complex as required. For example, you might use the if this policy is applied then > don't process anymore Auto Responder policies option to prevent more than one policy being applied. Conversely, you might define a policy to select a specific group of users and then use the if this policy is not applied then > process the next policy as a way of excluding groups of users without the need to add multiple exceptions.

Adding Auto Responder Policies

Policies are added using the new Auto Responder policy wizard - a series of screens which guide you through the setup process one step at a time.

The new Auto Responder policy wizard can be accessed from the console tree [see page 20], from the console toolbar [see page 19] and from the actions pane [see page 21]:



When the new option is selected, the new Auto Responder policy wizard is launched with a welcome page, followed by a list of available scenarios from which you can choose the type of policy to be created.

However, if you know the type of policy required before you start, it can be quicker to select the appropriate scenario from the new policy scenarios section of the actions pane. Once a policy scenario is selected, the new Auto Responder policy wizard is launched but initial welcome pages are skipped.

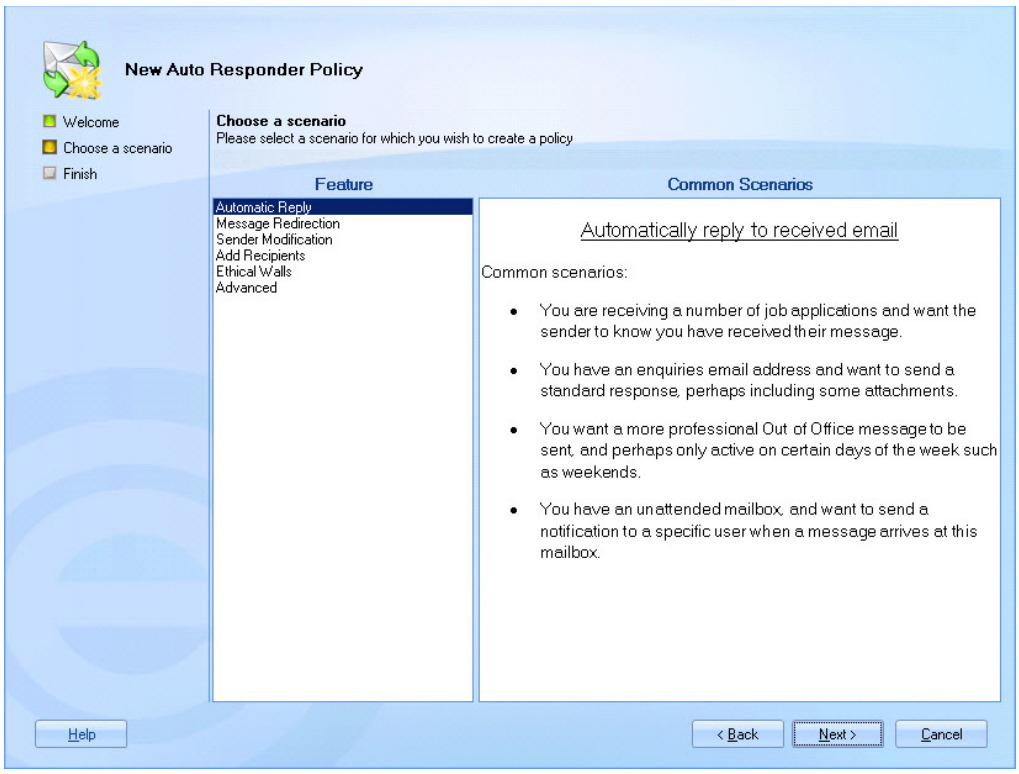
Adding an Automatic Reply Policy

To add an automatic reply [see page 60] policy, follow the steps below:

1. Select the Auto Responder policies branch of the console tree.
2. Select the new policy option from the actions pane to launch the new Auto Responder policy wizard at the welcome page.

> The **new policy** option is also available using the right-click menu or from the toolbar. Alternatively, you can use the **new policy scenarios** section of the **actions** pane to select a specific policy type. If you start with a specific scenario, the **welcome** page is not displayed - go straight to step 5.

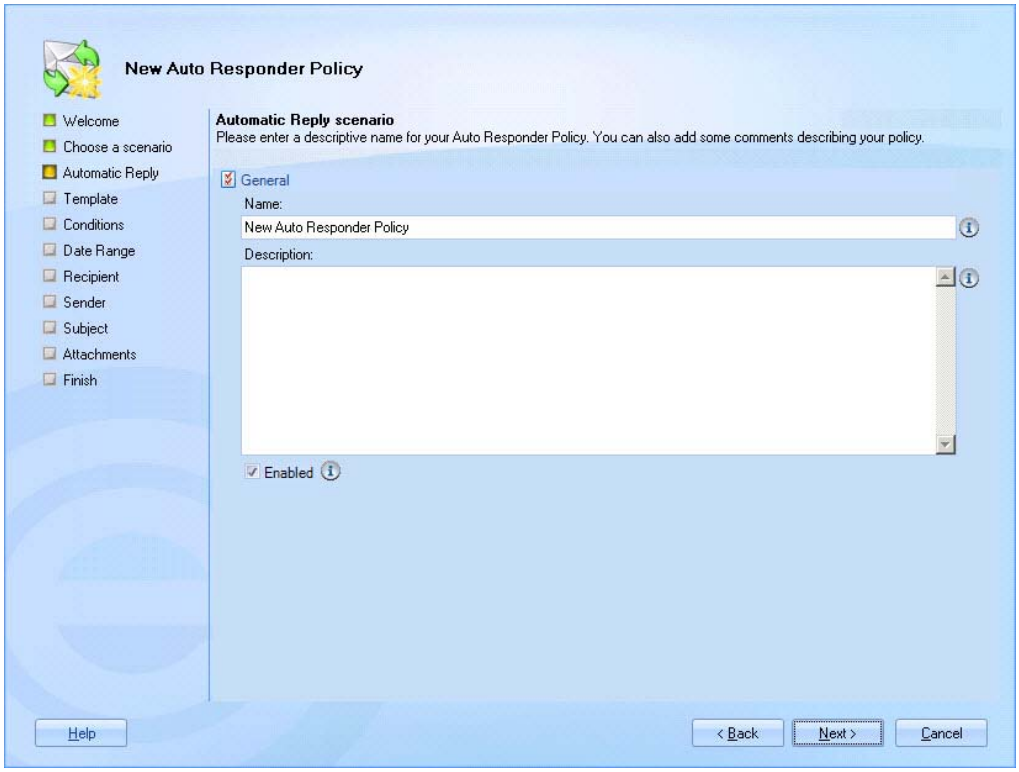
3. Click next to choose a scenario.



Here, available scenarios (policy types [see page 60]) are listed - if you are not sure what type of policy best suits your needs, you can select a scenario from the feature list and view summary information for each one.

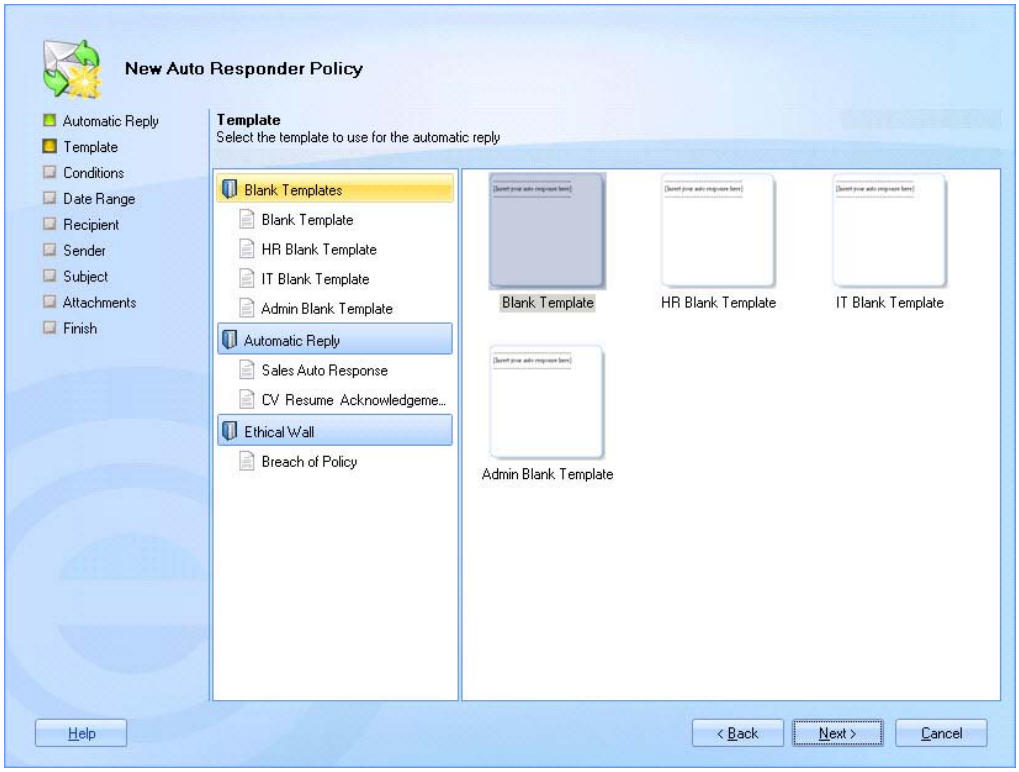
> If you started by choosing to create a specific scenario (via the actions pane), the **choose a scenario** page is not displayed - go straight to step 5.

4. Select the automatic reply scenario and click next to enter general information for the new policy:



5. Enter a meaningful name and description for the policy. For further information about this tab see anatomy of a policy - general on page 73.

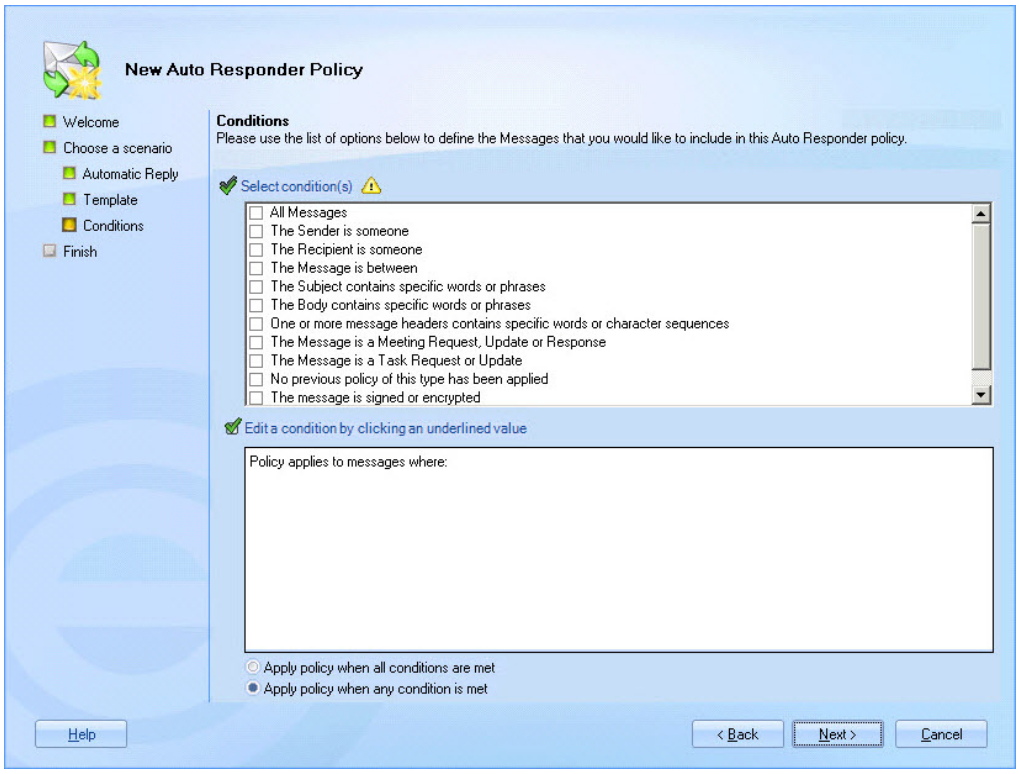
6. Click next to view available templates:



Here, you can browse all available templates and select the one that should be used for your automatic reply. If you can't find a template that meets your exact requirements, select any entry to complete the wizard.

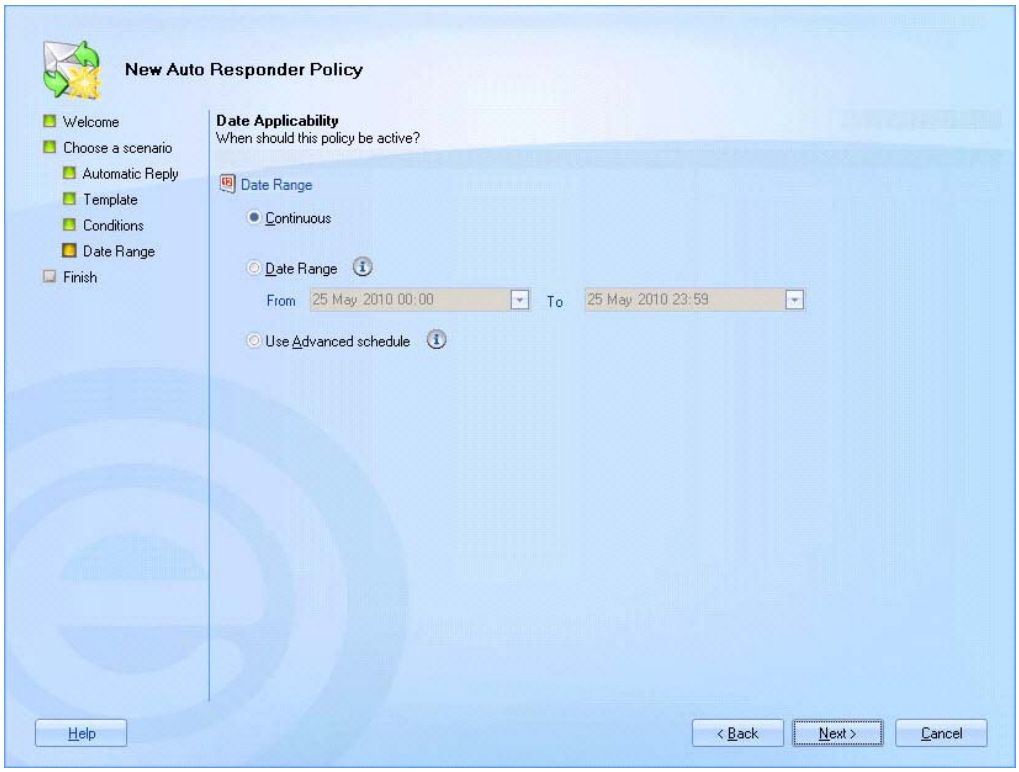
Later, you can use the template editor [see page 184] to create a more suitable template and then edit the policy [see page 179] to associate it with your new template [see page 132]. For further information about these options see anatomy of a policy - template on page 83.

7. Having selected the required template, click next to view conditions:



8. Set criteria [see page 85] to determine the circumstances under which an automatic reply is sent (you can update the conditions at any time, and also add exceptions [see page 91]). For further information about these options see anatomy of a policy - conditions on page 84.

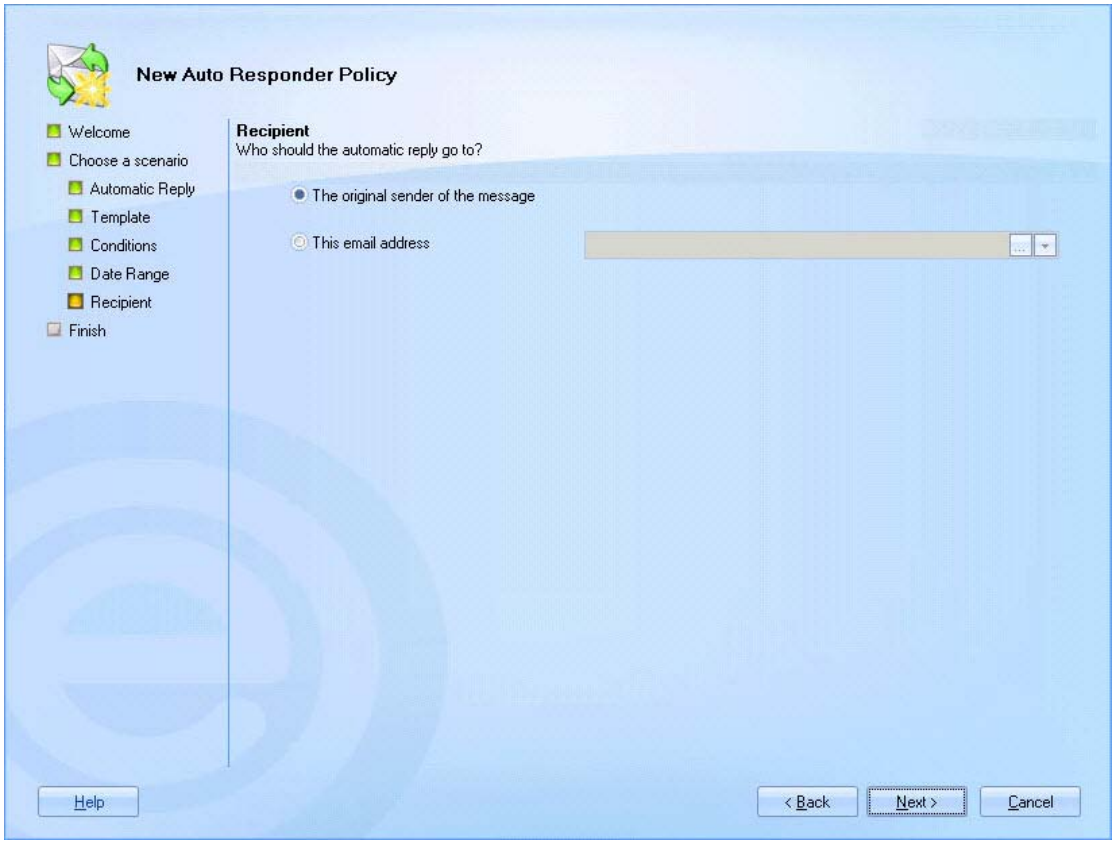
9. Click next to access date options for the policy:



The default setting is continuous which means that the policy will be processed from now, indefinitely. If preferred, you can choose to limit the policy to a given date range. For further information about these options see anatomy of a policy - date range on page 96.

10. If required, use the advanced schedule [see page 97] to set more specific times (within which the policy should be active). For further information about these options see advanced schedule on page 97.

11. Click next to access recipient options and specify who the automatic reply should be sent to:

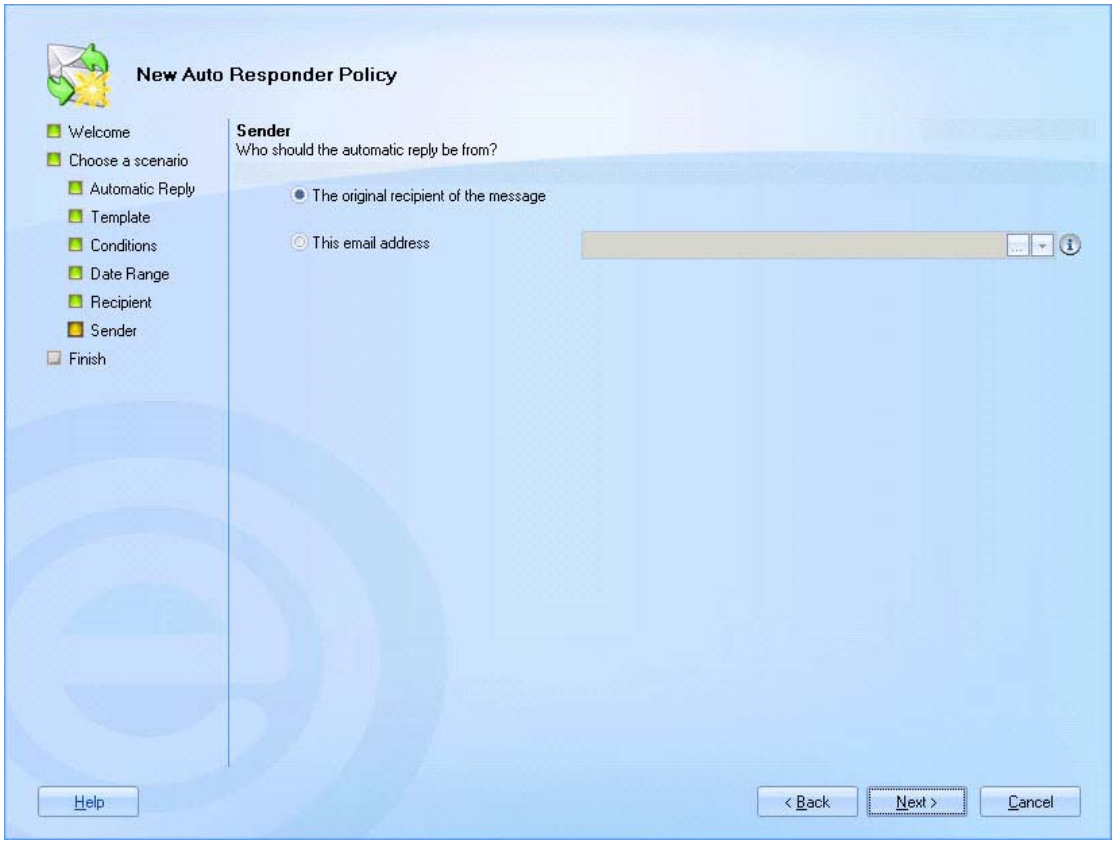


If you wish to send the automated response to the person who sent the original message, select the original sender of the message radio button. Alternatively, select the this email address option and add a specific email address.

You can type the required value directly into the associated field, use the browse button to browse user accounts and domains or use the arrow to select an Active Directory field [see page 198] from a drop-down list.

Any fields that are associated with email message [see page 201], message recipient [see page 209] and message sender [see page 202] details are available for selection. For further information about these options see anatomy of a policy - auto response on page 78.

12. Click next to access sender options and specify who the automatic reply should be from:

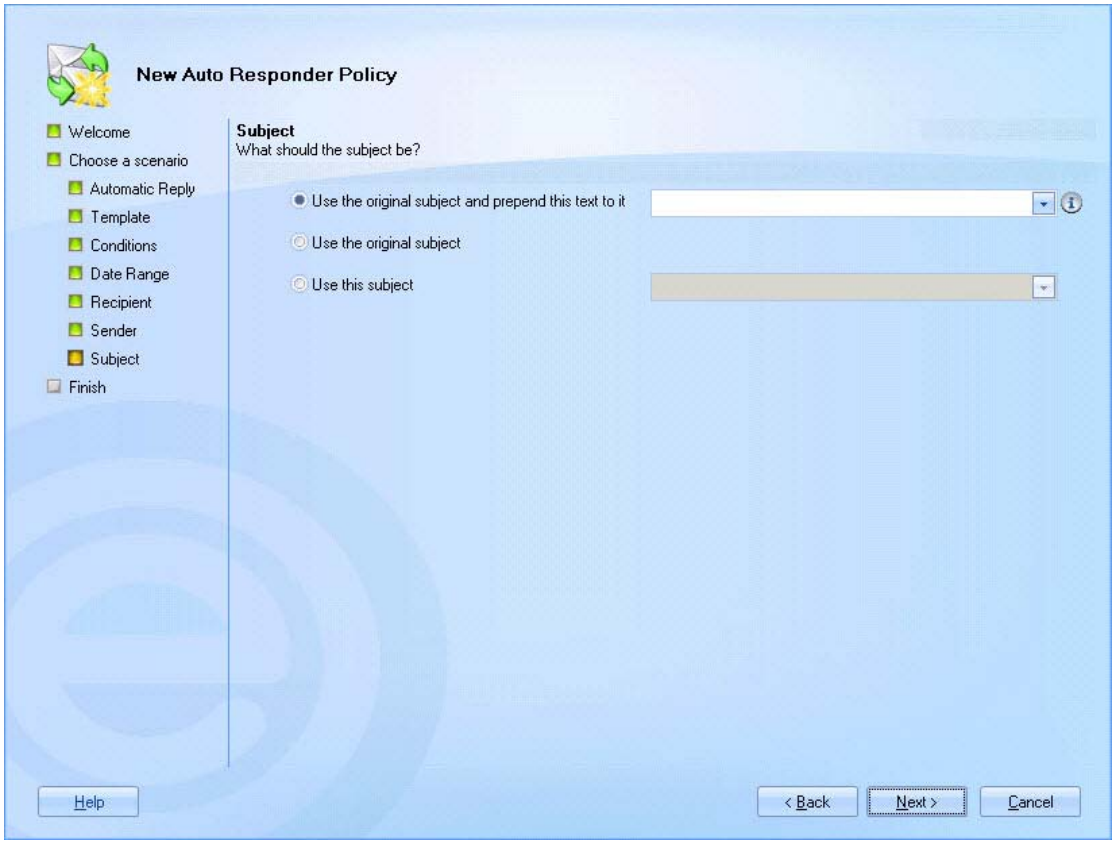


If you wish the original message recipient to be shown in the from field of the automatic reply, select the original recipient of the message option. Alternatively, select the this email address option and add a specific email address.

You can type the required value directly into the associated field, use the browse button to browse user accounts and domains or use the arrow to select an Active Directory field [see page 198] from a drop-down list. Any fields that are associated with email message [see page 201], message recipient [see page 209] and message sender [see page 202] details are available for selection.

For further information about these options see anatomy of a policy - auto response on page 78.

13. Click next to access subject options and specify what information to show in the subject line of the automatic reply message:



By default this field is set to use the original subject and prepend this text to it. Here, you can enter required text to show before the original subject (for example, RE:).

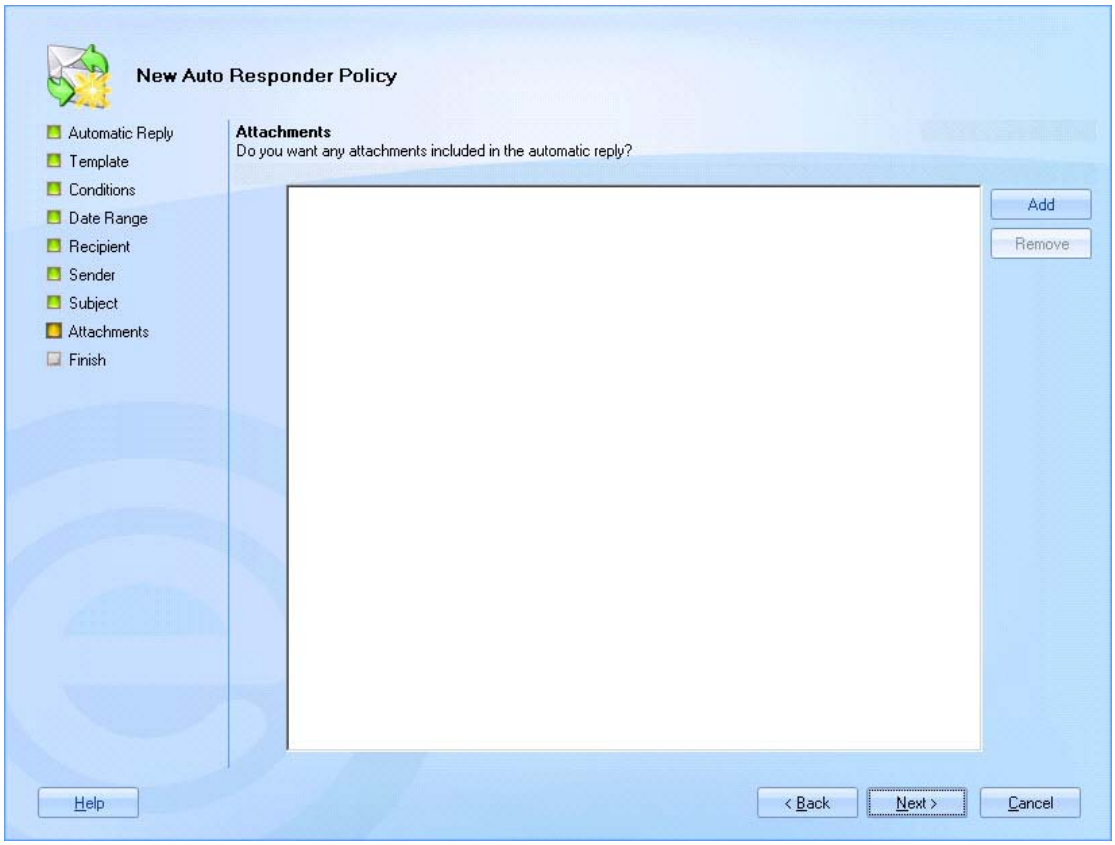
If you simply want to use the original subject (without any prepended text), select the use the original subject option. Alternatively, you can specify a new subject line for the automatic reply.

Select the use this subject option and enter any static text and/or use the arrow to select a field [see page 198] from a drop-down list. Any fields that are associated with email message [see page 201], recipient [see page 209], sender [see page 202], dynamic content [see page 215], server [see page 224] and general [see page 224] details are available for selection.

For example, you might define a subject line which reads 'Re. your message sent to Joe Bloggs' where 'Joe Bloggs' is dynamically replaced with the original message recipient name. To achieve this, you would type: Re. your message sent to and then insert the message recipients field:

For further information about these options see anatomy of a policy - auto response on page 78.

14. Click next to access attachments options:



If you wish to send any attachments with the automatic reply, click the add button, then navigate local / network drives to select the required file(s).

15. Click next to confirm your selections and access the final page of the wizard.

16. Click finish to complete the process and add the new policy to the policies list [see page 67].

> You must click the **save** button at the top of the Exclaimer console to save changes in Auto Responder. If you do not save changes (or if you use the **cancel** button) the new policy will not be retained when you exit from Auto Responder.

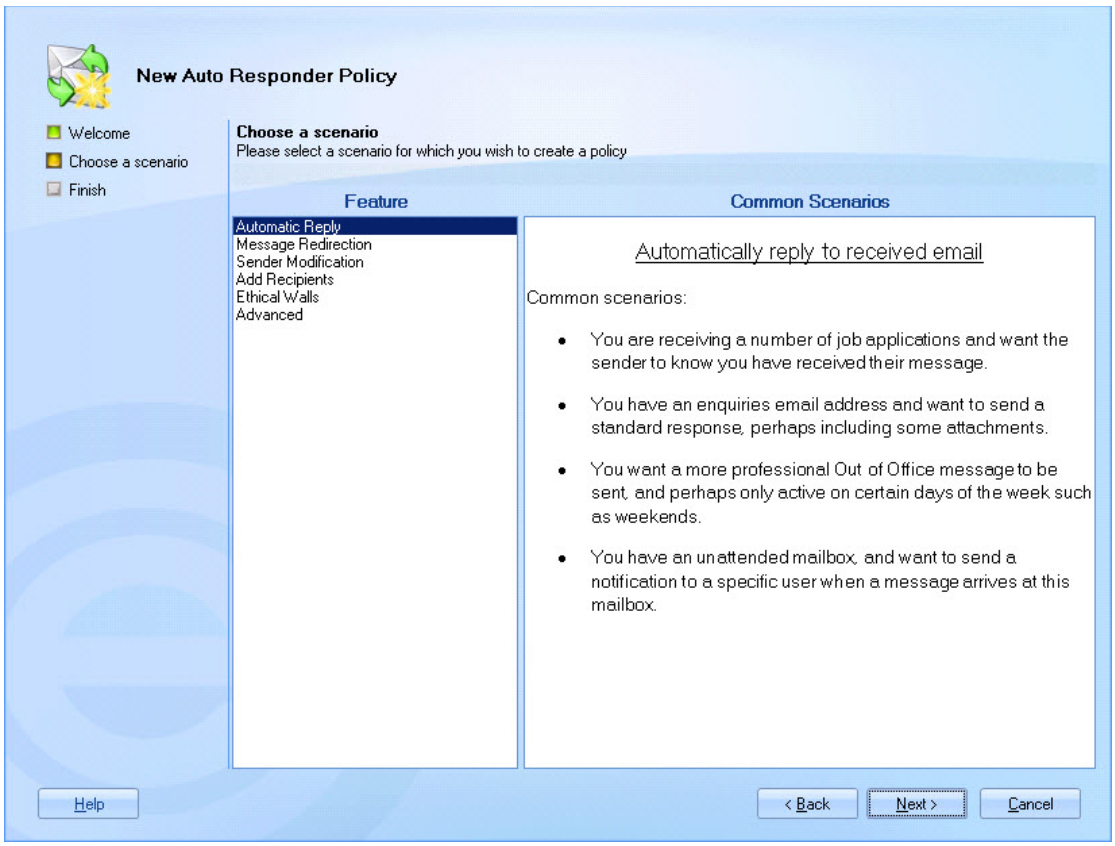
Adding a Message Redirection Policy

To add a message redirection [see page 61] policy, follow the steps below:

1. Select the Auto Responder policies branch of the console tree.
2. Select the new policy option from the actions pane to launch the new Auto Responder policy wizard at the welcome page.

> The **new policy** option is also available using the right-click menu or from the toolbar. Alternatively, you can use the **new policy scenarios** section of the **actions** pane to select a specific policy type. If you start with a specific scenario, the **welcome** page is not displayed - go straight to step 5.

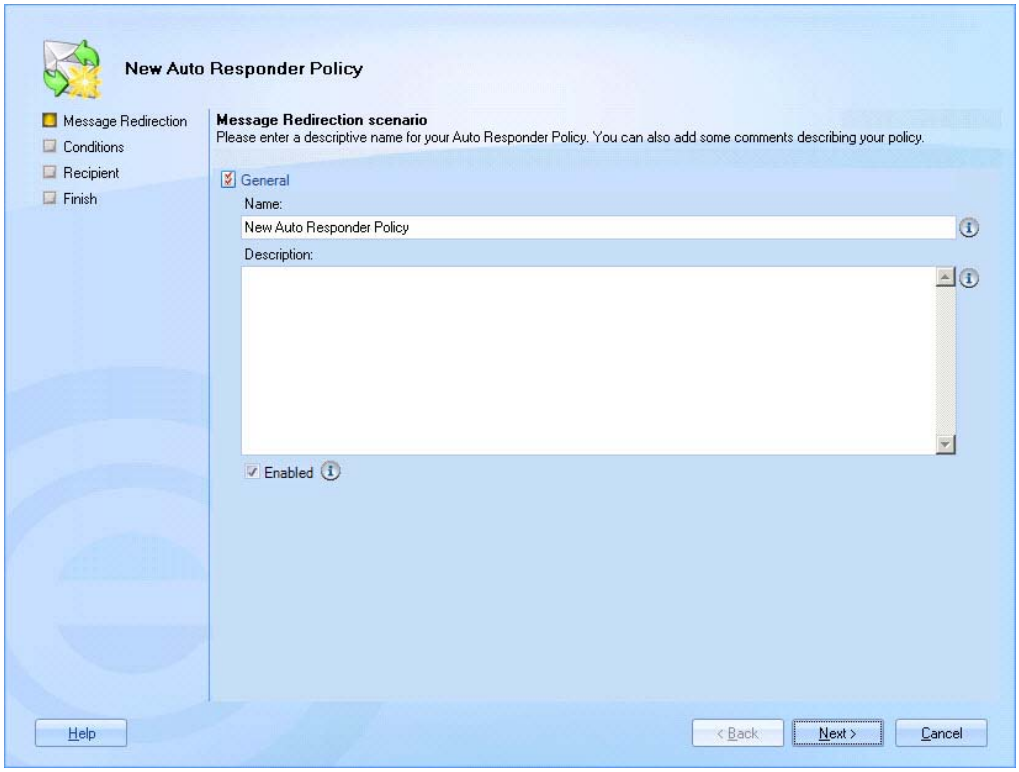
3. Click next to choose a scenario:



Here, available scenarios (policy types [see page 60]) are listed - if you are not sure what type of policy best suits your needs, you can select a scenario from the feature list and view summary information for each one.

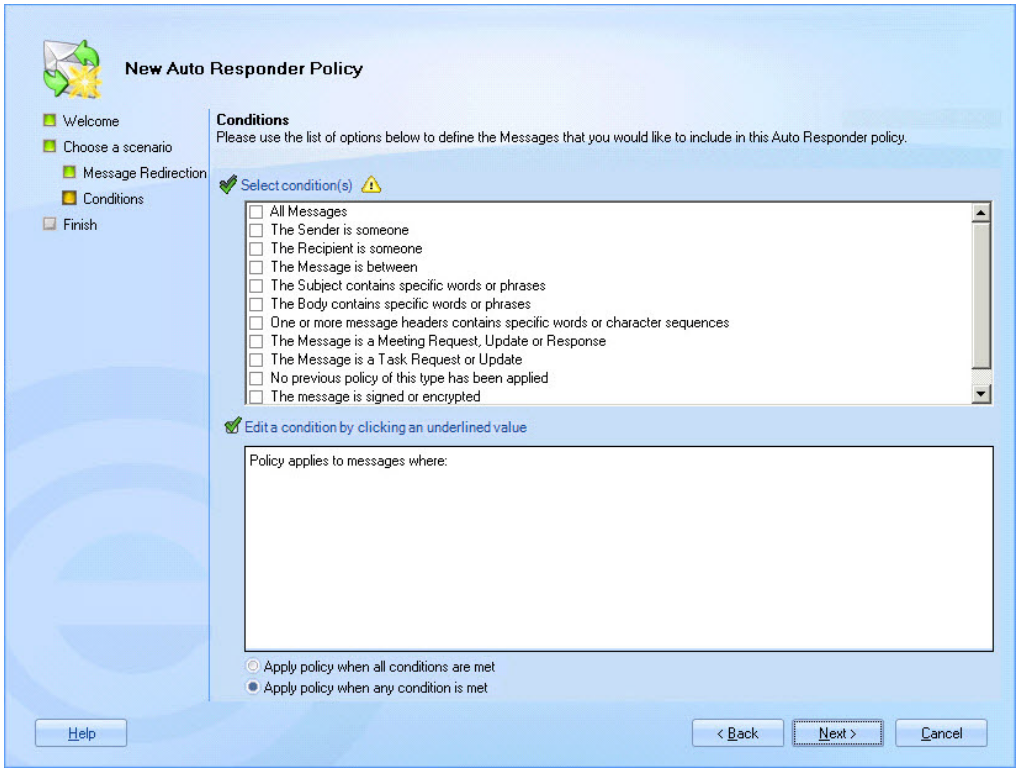
> If you started by choosing to create a specific scenario (via the actions pane), the **choose a scenario** page is not displayed - go straight to step 5.

4. Select the message redirection scenario and click next to enter general information for the new policy:



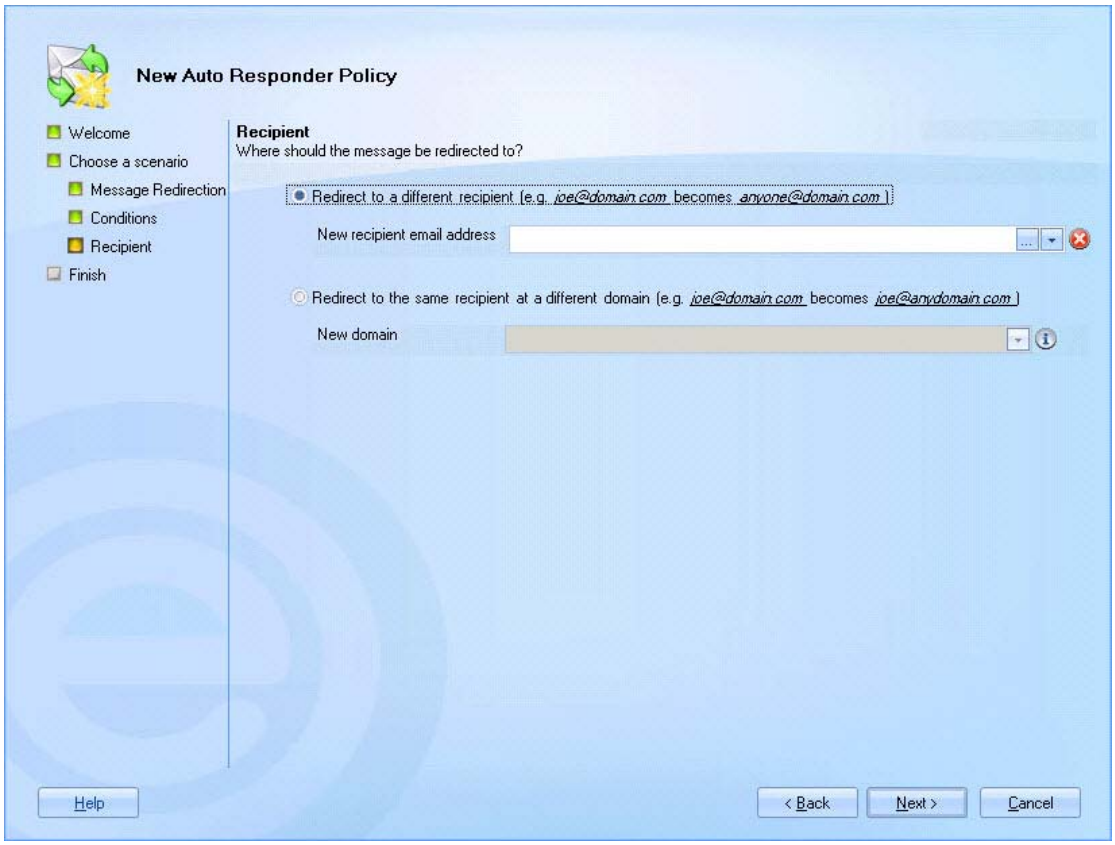
5. Enter a meaningful name and description for the policy. For further information about this tab see anatomy of a policy - general on page 73.

6. Click next to view conditions:



7. Set criteria [see page 85] to determine the circumstances under which the policy is applied and messages are redirected. Having created the policy, you can update the conditions at any time, and also add exceptions [see page 91]. For further information about these options see anatomy of a policy - conditions on page 84.

8. Click next to access recipient options:



Here, you can specify email addresses to which messages should be redirected. If you choose to redirect to a different user and specify an email address, any recipients specified in the original message are ignored and the message is redirected to the address specified here.

If you choose to redirect to the same recipient at a different domain, the local part of the email address would remain the same but the domain would be changed. For example, joe.bloggs@domain1.com might be changed to joe.bloggs@domain2.com. For further information about these options see anatomy of a policy - original message on page 74.

When choosing to add addresses you can type the required value directly into the associated field. Alternatively, you can use the browse button to browse user accounts and domains, or use the arrow to select an Active Directory field [see page 198] from a drop-down list. Any fields that are associated with email message [see page 201] and message sender [see page 202] details are available for selection.

9. Click next to confirm your selections and access the final page of the wizard.

10. Click finish to complete the process and add the new policy to the policies list [see page 67].

> You must click the **save** button at the top of the Exclaimer console to save changes in Auto Responder. If you do not save changes (or if you use the **cancel** button) the new policy will not be retained when you exit from Auto Responder.

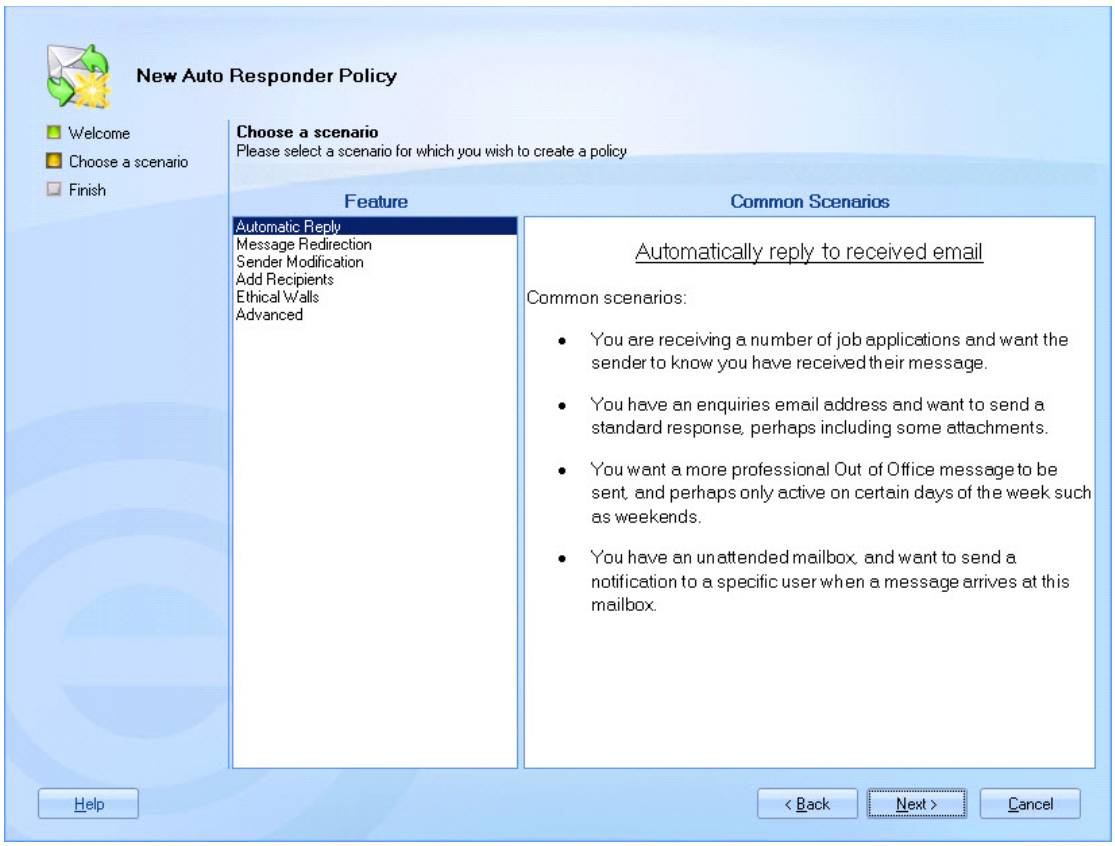
Adding a Sender Modification Policy

To add a sender modification [see page 61] policy, follow the steps below:

1. Select the Auto Responder policies branch of the console tree.
2. Select the new policy option from the actions pane to launch the new Auto Responder policy wizard at the welcome page.

> The **new policy** option is also available using the right-click menu or from the toolbar. Alternatively, you can use the **new policy scenarios** section of the **actions** pane to select a specific policy type. If you start with a specific scenario, the **welcome** page is not displayed - go straight to step 5.

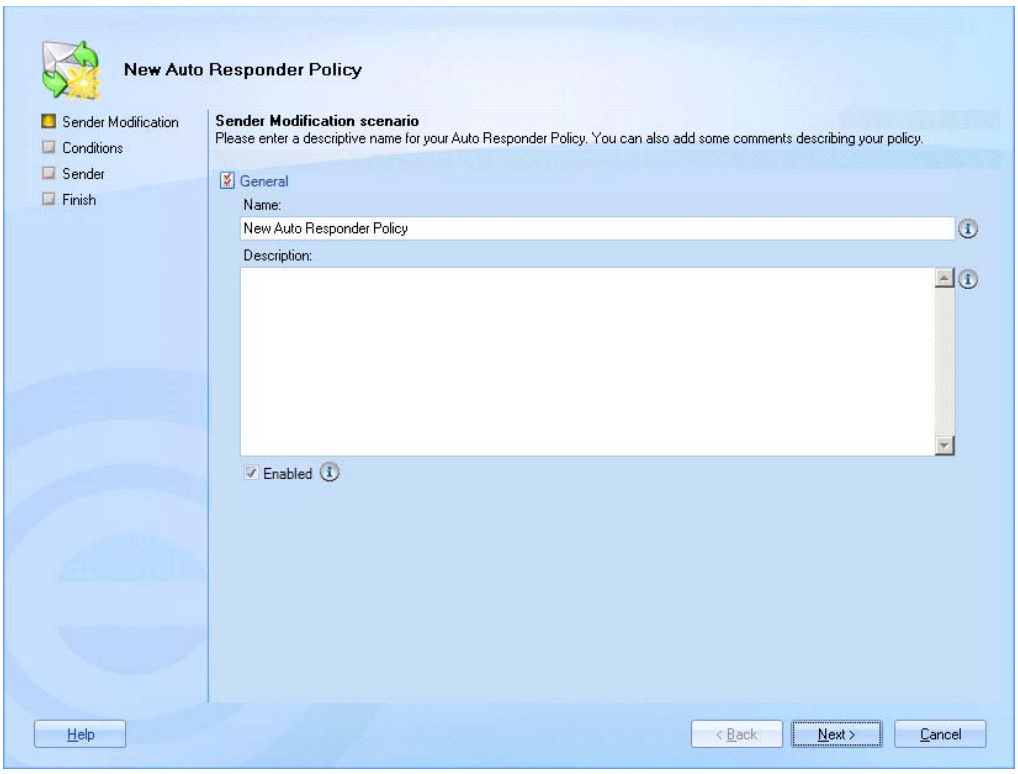
3. Click next to choose a scenario:



4. Here, available scenarios (policy types [see page 60]) are listed - if you are not sure what type of policy best suits your needs, you can select a scenario from the feature list and view summary information for each one.

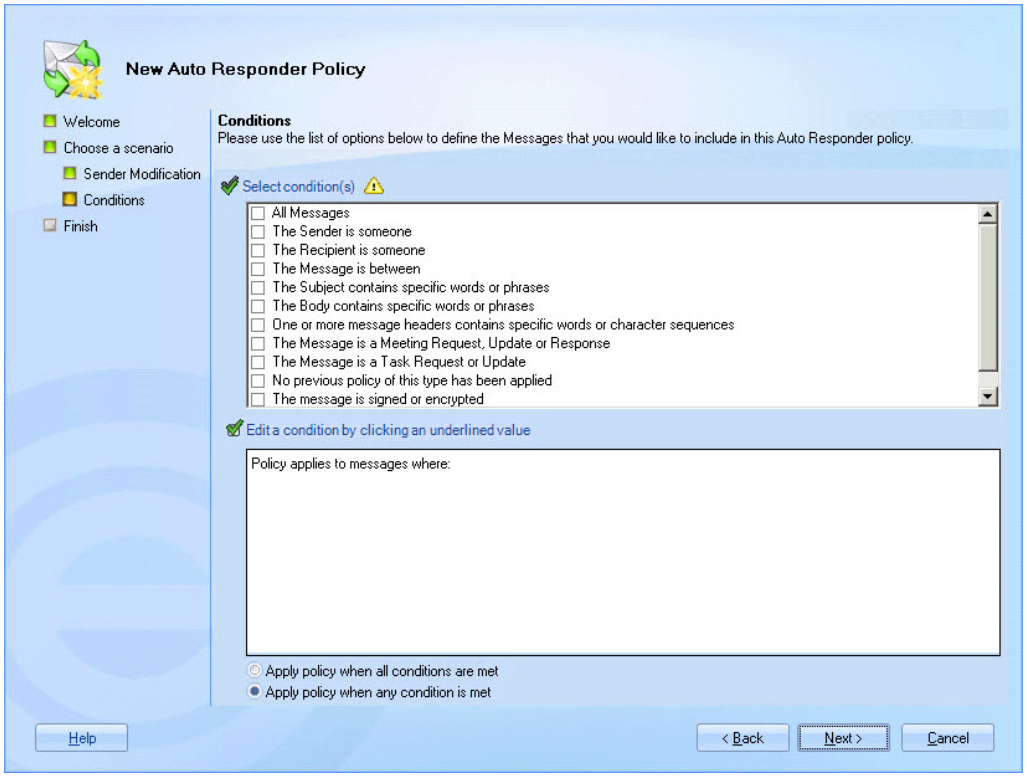
> If you started by choosing to create a specific scenario (via the actions pane), the **choose a scenario** page is not displayed - go straight to step 5.

5. Select the sender modification scenario and click next to enter general information for the new policy:



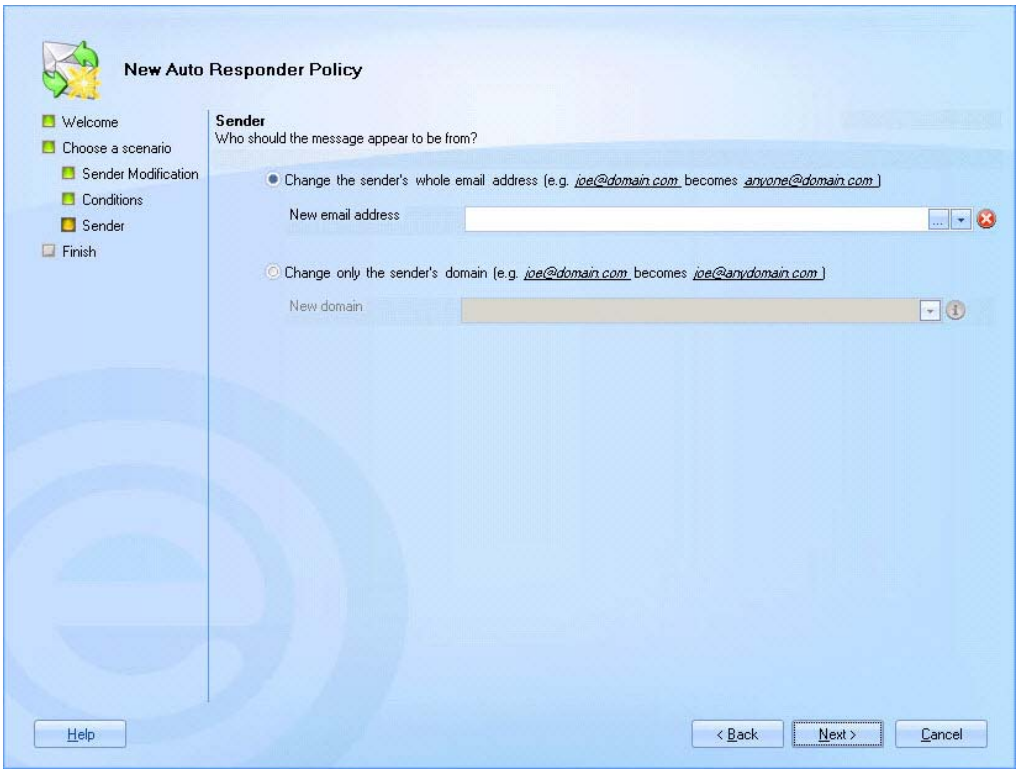
6. Enter a meaningful name and description for the policy. For further information about this tab see anatomy of a policy - general on page 73.

7. Click next to view conditions:



8. Set criteria [see page 85] to determine the circumstances under which the policy is applied and sender details are modified. Having created the policy, you can update the conditions at any time, and also add exceptions [see page 91]. For further information about these options see anatomy of a policy - conditions on page 84.

9. Click next to access sender options:



If you choose to change the sender's whole email address and specify a new address, this will be displayed in the from field of the email when the message is received.

Alternatively, you can choose to change only the sender's domain (for example, if you are phasing out an old domain). When this option is selected, the local part of the email address would remain the same but the domain would be changed. For example, joe.bloggs@domain1.com might be changed to joe.bloggs@domain2.com.

For further information about these options see anatomy of a policy - original message on page 74.

When choosing to add addresses you can type the required value directly into the associated field. Alternatively, you can use the browse button to browse user accounts and domains, or use the arrow to select an Active Directory field [see page 198] from a drop-down list. Any fields that are associated with email message [see page 201], message sender [see page 202], server [see page 224] and general [see page 224] details are available for selection.

10. Click next to confirm your selections and access the final page of the wizard.

11. Click finish to complete the process and add the new policy to the policies list [see page 67].

You must click the **save** button at the top of the Exclaimer console to save changes in Auto Responder. If you do not save changes (or if you use the **cancel** button) the new policy will not be retained when you exit from Auto Responder.

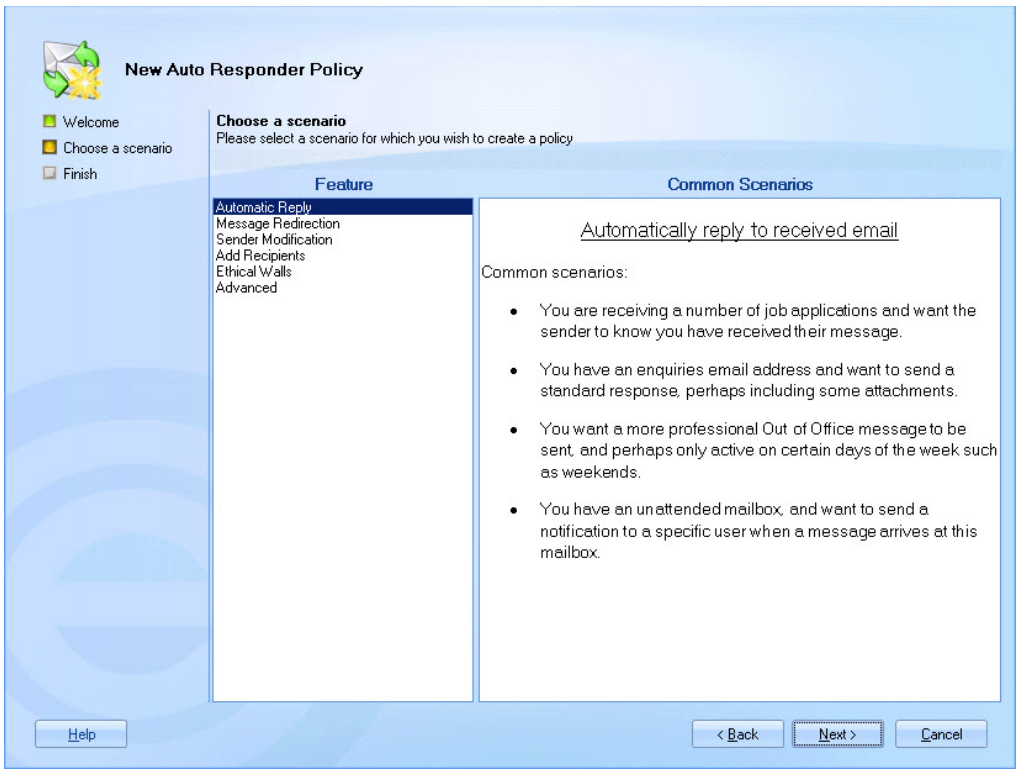
Adding an Add Recipients Policy

To add an add recipients [see page 62] policy, follow the steps below:

1. Select the Auto Responder policies branch of the console tree.
2. Select the new policy option from the actions pane to launch the new Auto Responder policy wizard at the welcome page.

> The **new policy** option is also available using the right-click menu or from the toolbar. Alternatively, you can use the **new policy scenarios** section of the **actions** pane to select a specific policy type. If you start with a specific scenario, the **welcome** page is not displayed - go straight to step 5.

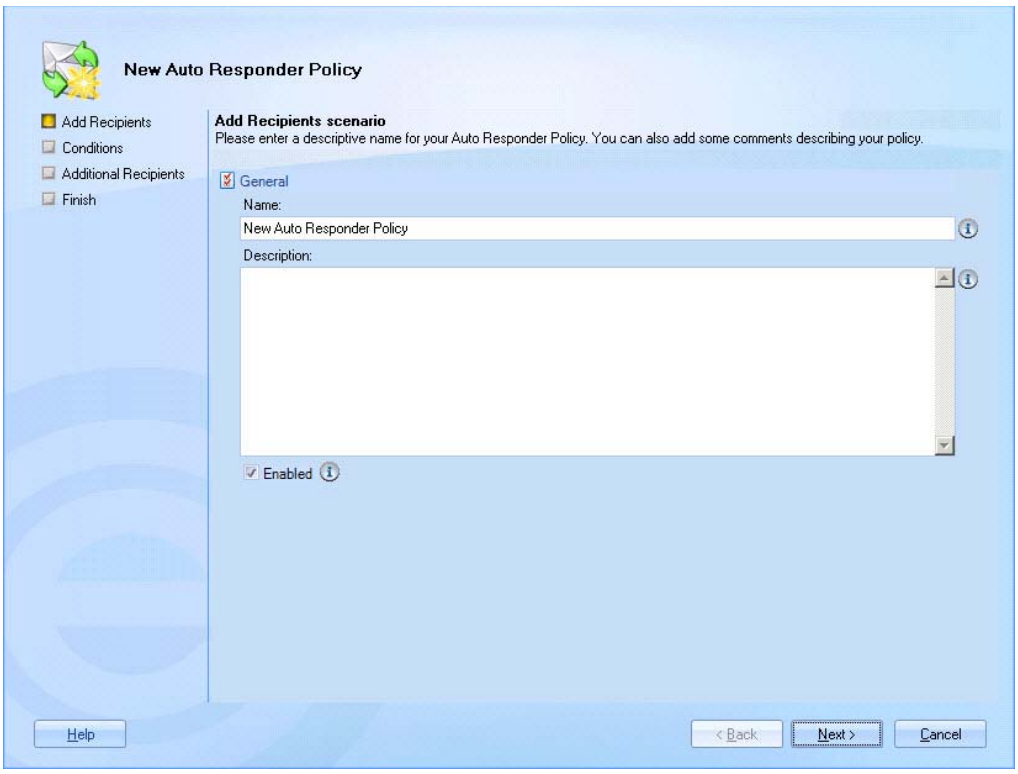
3. Click next to choose a scenario:



4. Here, available scenarios (policy types [see page 60]) are listed - if you are not sure what type of policy best suits your needs, you can select a scenario from the feature list and view summary information for each one.

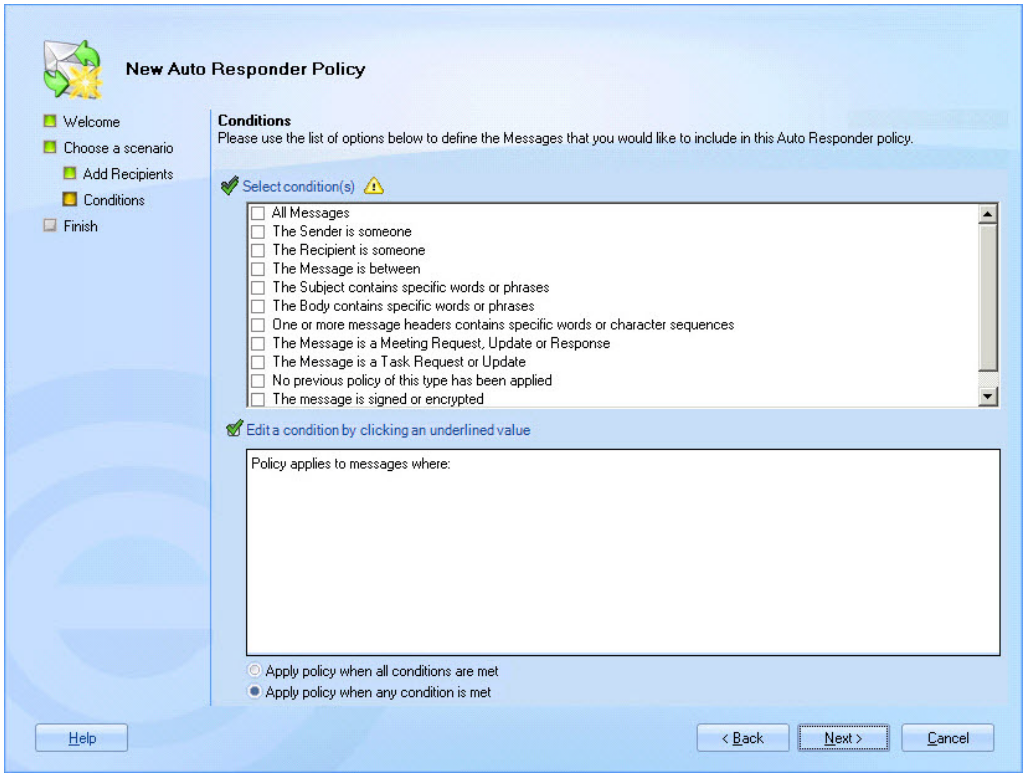
> If you started by choosing to create a specific scenario (via the actions pane), the **choose a scenario** page is not displayed - go straight to step 5.

5. Select the add recipients scenario and click next to enter general information for the new policy:



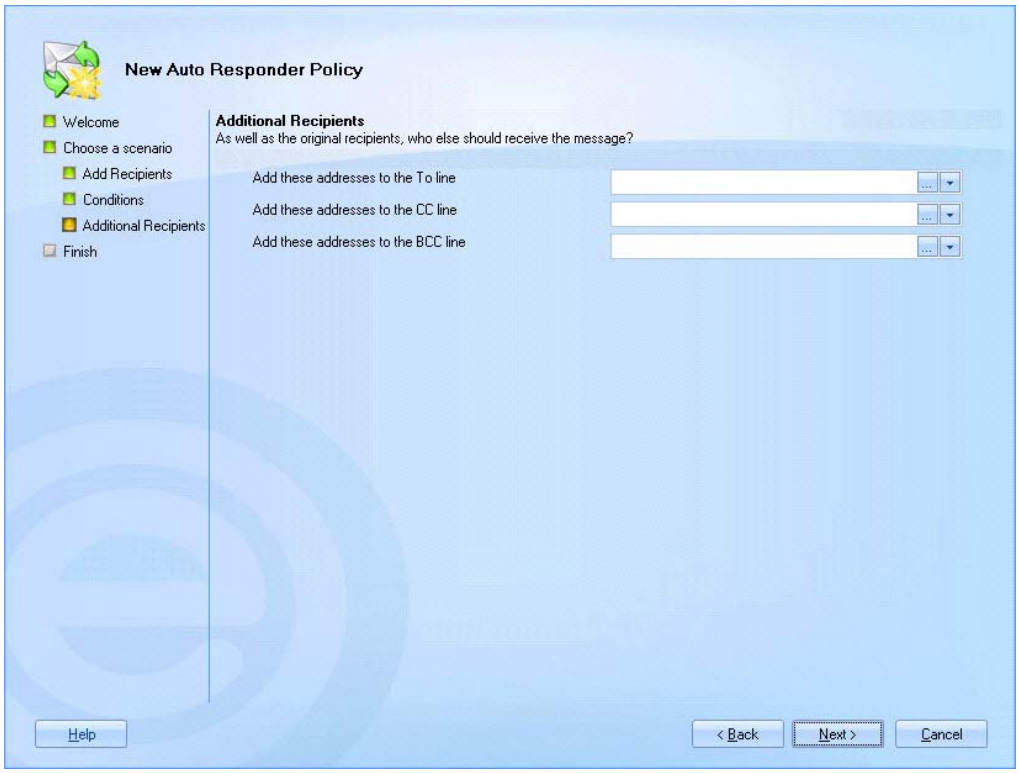
6. Enter a meaningful name and description for the policy. For further information about this tab see anatomy of a policy - general on page 73.

7. Click next to view conditions:



8. Set criteria [see page 85] to determine the circumstances under which the policy is applied and recipients are added. Having created the policy, you can update the conditions at any time, and also add exceptions [see page 91]. For further information about these options see anatomy of a policy - conditions on page 84.

9. Click next to access additional recipients options:



Here, you can specify email addresses to be added as recipients in to, CC and BCC fields.

When choosing to add addresses you can type the required value directly into the associated field, use the browse button to browse user accounts and domains or use the arrow to select an Active Directory field [see page 198] from a drop-down list. Any fields that are associated with email message [see page 201], message recipient [see page 209] and message sender [see page 202] details are available for selection.

For further information about these options see anatomy of a policy - auto response on page 78.

10. Click next to confirm your selections and access the final page of the wizard.

11. Click finish to complete the process and add the new policy to the policies list [see page 67].

> You must click the **save** button at the top of the Exclaimer console to save changes in Auto Responder. If you do not save changes (or if you use the **cancel** button) the new policy will not be retained when you exit from Auto Responder.

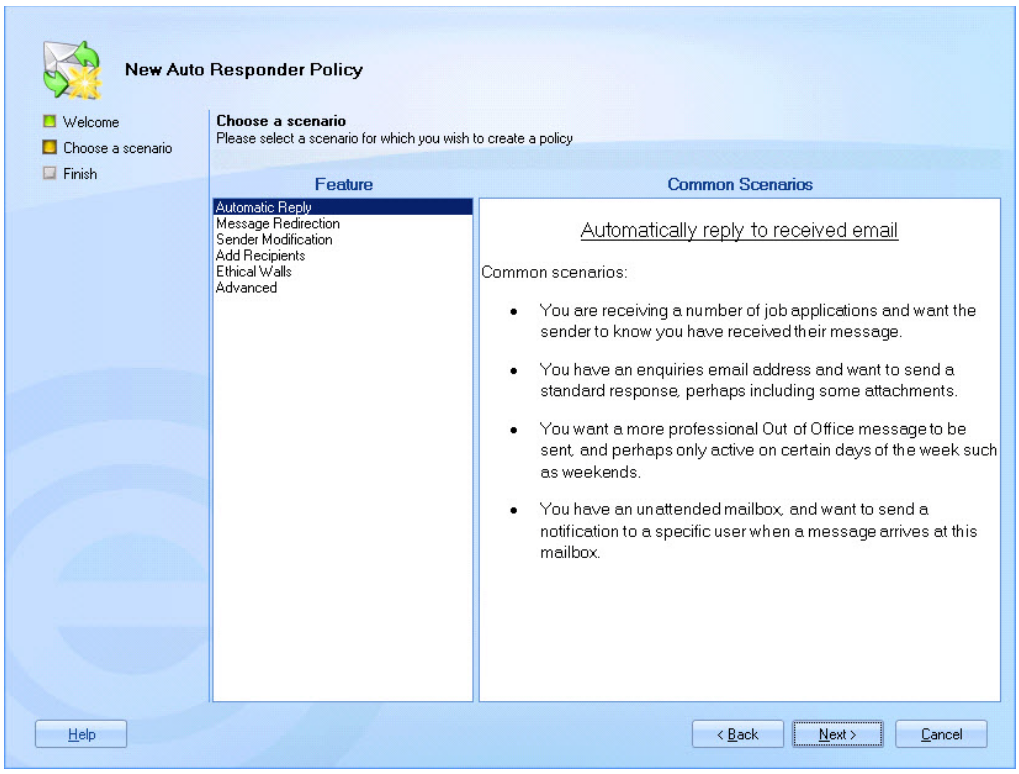
Adding an Ethical Walls Policy

To add an ethical walls [see page 62] policy, follow the steps below:

1. Select the Auto Responder policies branch of the console tree.
2. Select the new policy option from the actions pane to launch the new Auto Responder policy wizard at the welcome page.

> The **new policy** option is also available using the right-click menu or from the toolbar. Alternatively, you can use the **new policy scenarios** section of the **actions** pane to select a specific policy type. If you start with a specific scenario, the **welcome** page is not displayed - go straight to step 5.

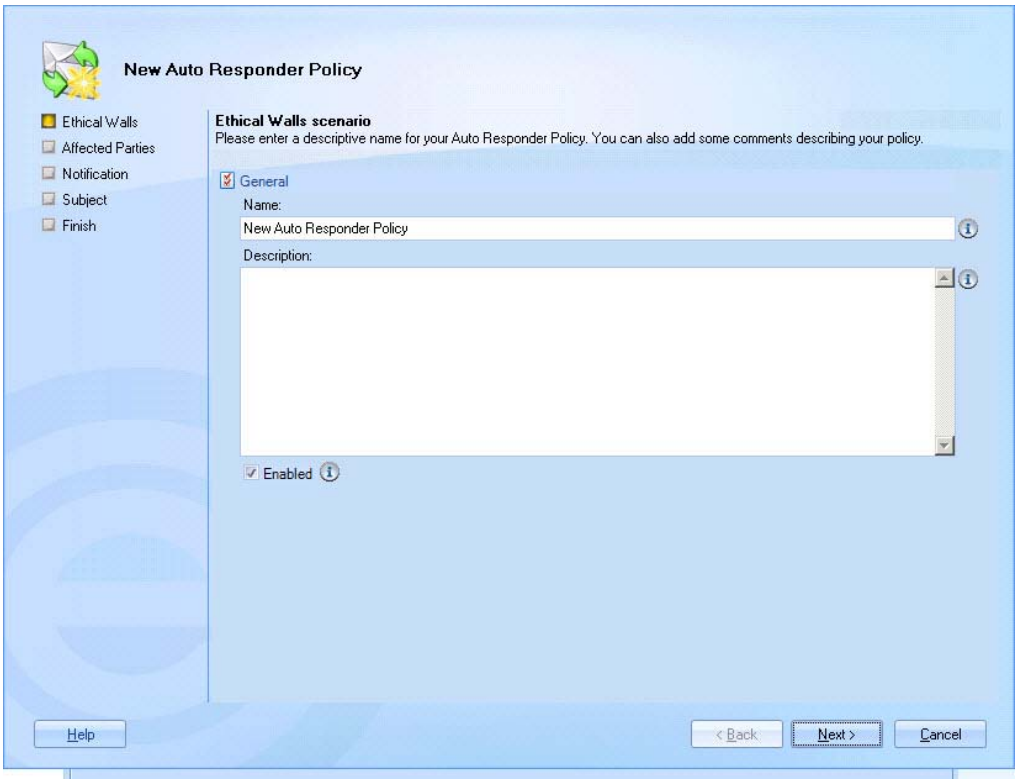
3. Click next to choose a scenario:



Here, available scenarios (policy types [see page 60]) are listed - if you are not sure what type of policy best suits your needs, you can select a scenario from the feature list and view summary information for each one.

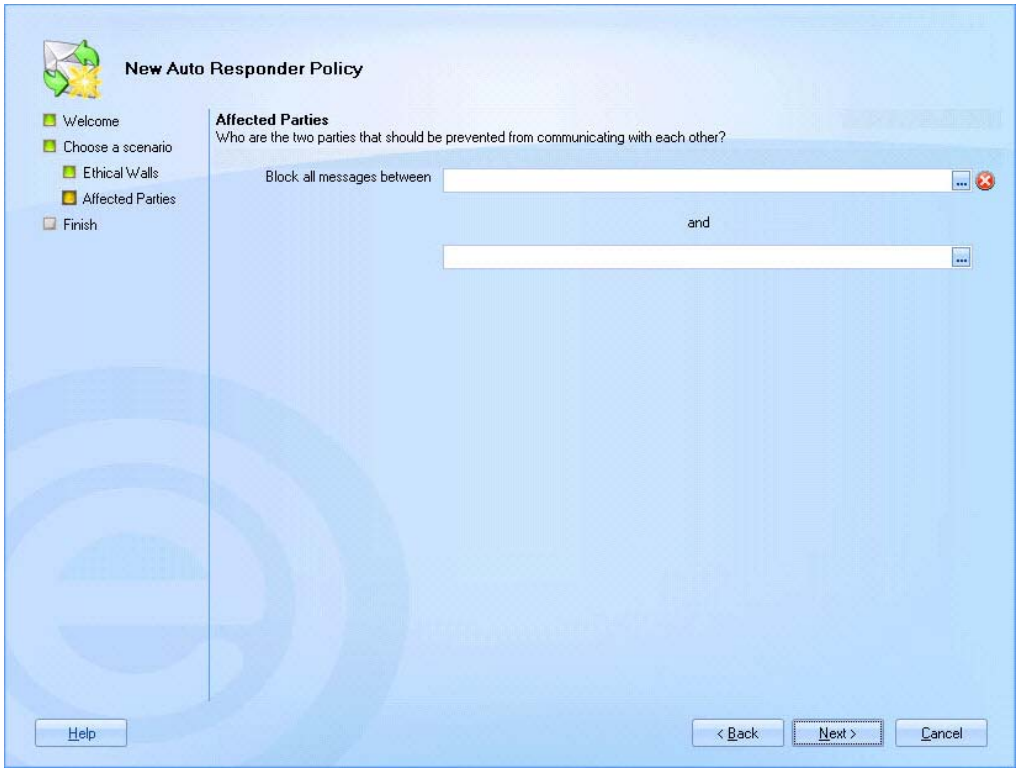
> If you started by choosing to create a specific scenario (via the actions pane), the **choose a scenario** page is not displayed - go straight to step 5.

4. Select the ethical walls scenario and click next to enter general information for the new policy:



5. Enter a meaningful name and description for the policy. For further information about this tab see anatomy of a policy - general on page 73.

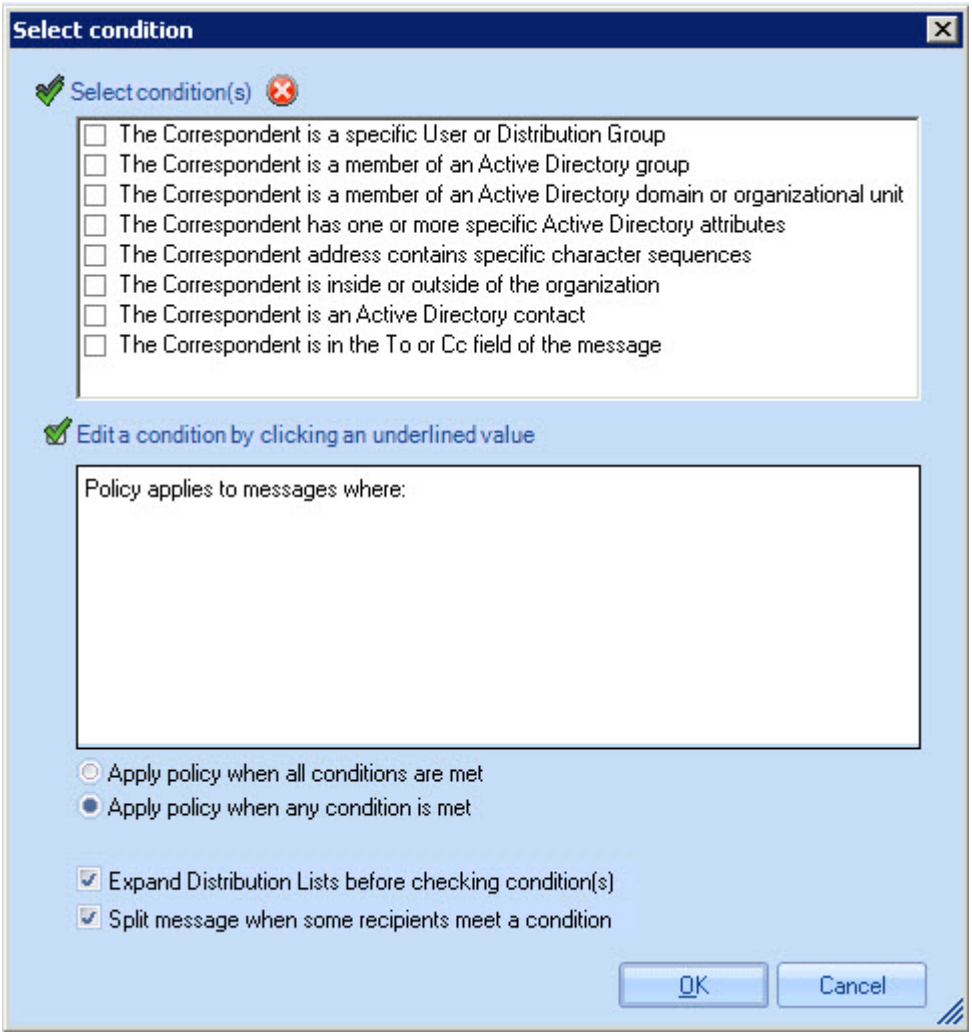
6. Click next to access affected parties options:



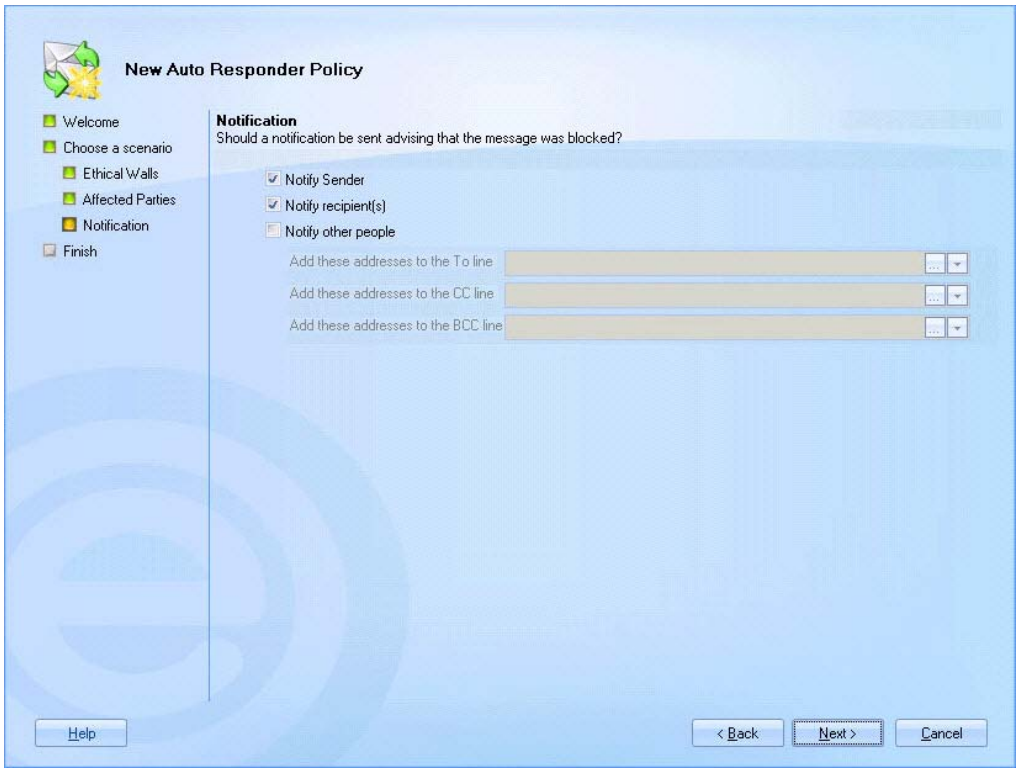
7. Here, you specify two parties between which email communication will be blocked. Use the browse button to browse and select from user accounts and groups.

   At this stage you must select affected parties from existing users and groups. Typically (though not always) ethical walls policies are defined to block communication between predefined groups. However, it is important to note that you can change / refine these settings once the policy is saved, using the conditions tab for the policy [see page 84].

   Having completed the wizard, the conditions [see page 84] tab for that policy will show your chosen affected parties under the message is between condition. You can change these parties at any stage - for example, you might choose to define affected parties based upon Active Directory attributes or recipient type (To or Cc), etc:

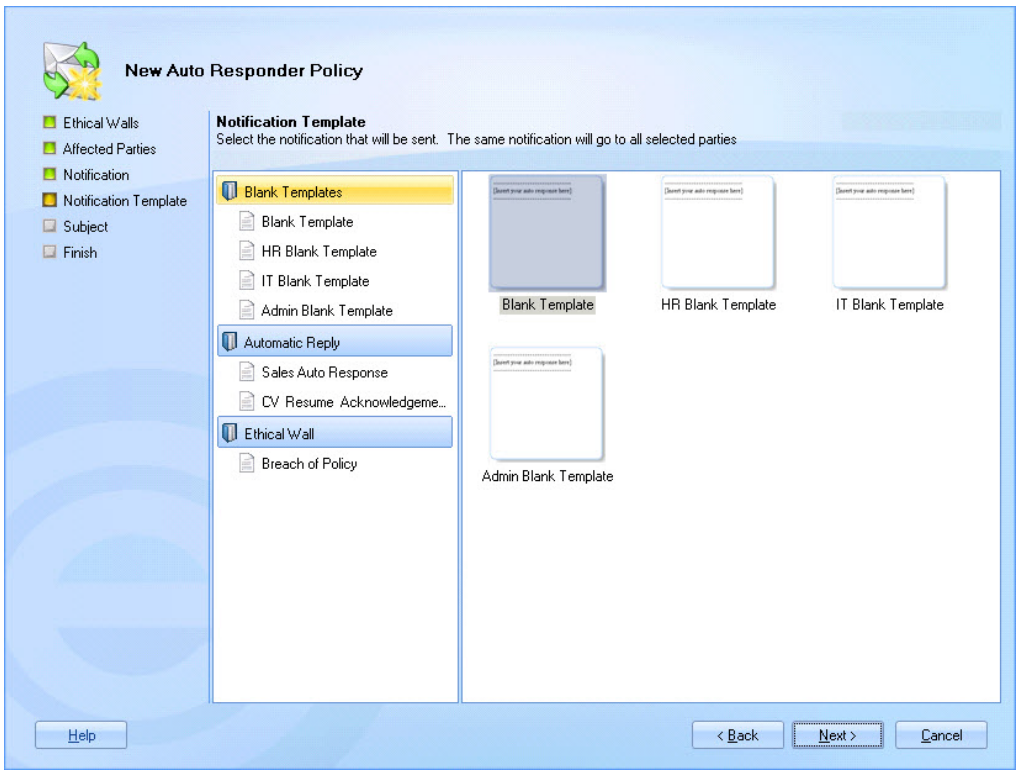


8. Click next to access notification options:



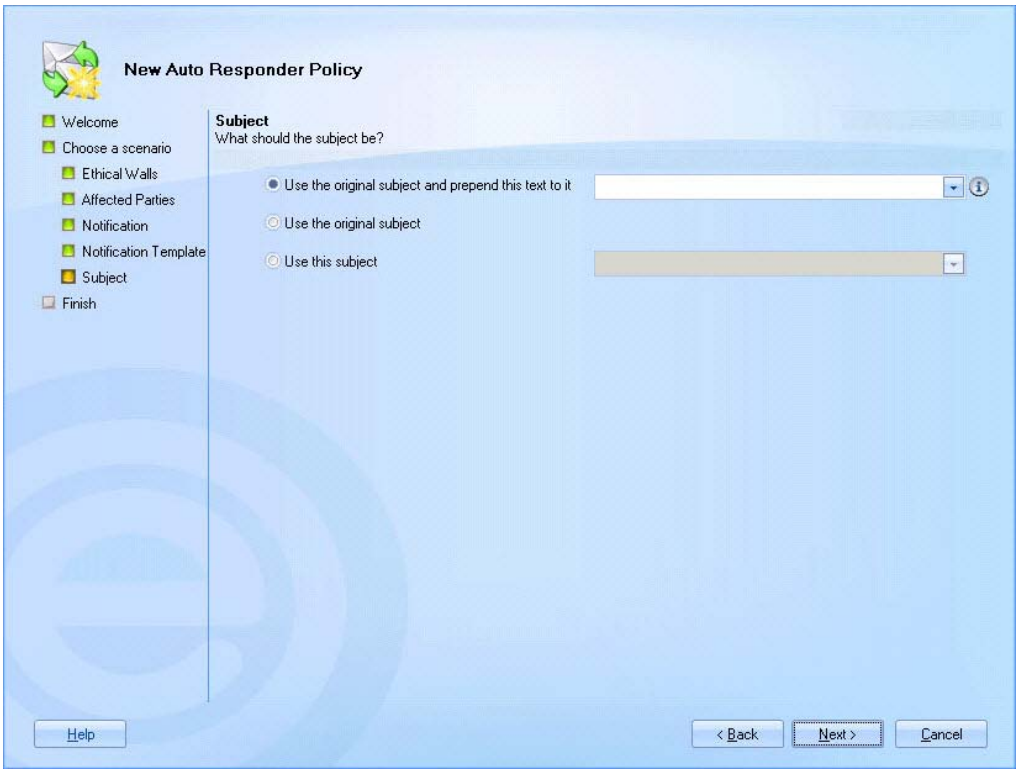
Here, you can choose to notify the original sender and / or recipients and / or other parties when an email (between the two specified accounts) has been blocked.

9. Click next. If you have chosen to send one or more notifications (in the previous step), the notification template page is displayed:



Here, you can browse all available templates and select the one that should be used for your notification message. If you can't find a template that meets your exact requirements, select any entry to complete the wizard. Later, you can use the template editor [see page 184] to create a more suitable template and then edit the policy [see page 179] to associate it with your new template [see page 132]. For further information about these options see anatomy of a policy - template on page 83.

10. Click next to access subject options and specify what information to show in the subject line of the notification message:



By default this field is set to use the original subject and prepend this text to it. Here, you can enter required text to show before the original subject (for example, RE:).

If you simply want to use the original subject (without any prepended text), select the use the original subject option. Alternatively, you can specify a new subject line for the automatic reply. Select the use this subject option and enter any static text and/or use the arrow to select a field [see page 198] from a drop-down list. Any fields that are associated with email message [see page 201], recipient [see page 209], sender [see page 202], dynamic content [see page 215], server [see page 224] and general [see page 224] details are available for selection.

For example, you might define a subject line which reads 'Re. your message sent to Joe Bloggs' where 'Joe Bloggs' is dynamically replaced with the original message recipient name. To achieve this, you would type: Re. your message sent to and then insert the message recipients field:

For further information about these options see anatomy of a policy - auto response on page 78.

11. Click next to confirm your selections and access the final page of the wizard.

12. Click finish to complete the process and add the new policy to the policies list [see page 67].

Remember that you can update conditions [see page 84] at any time, and also add exceptions [see page 91] or date range [see page 96] criteria, after the policy has been created.

Also note that you must click the **save** button at the top of the Exclaimer console to save changes in Auto Responder. If you do not save changes (or if you use the **cancel** button) the new policy will not be retained when you exit from Auto Responder.

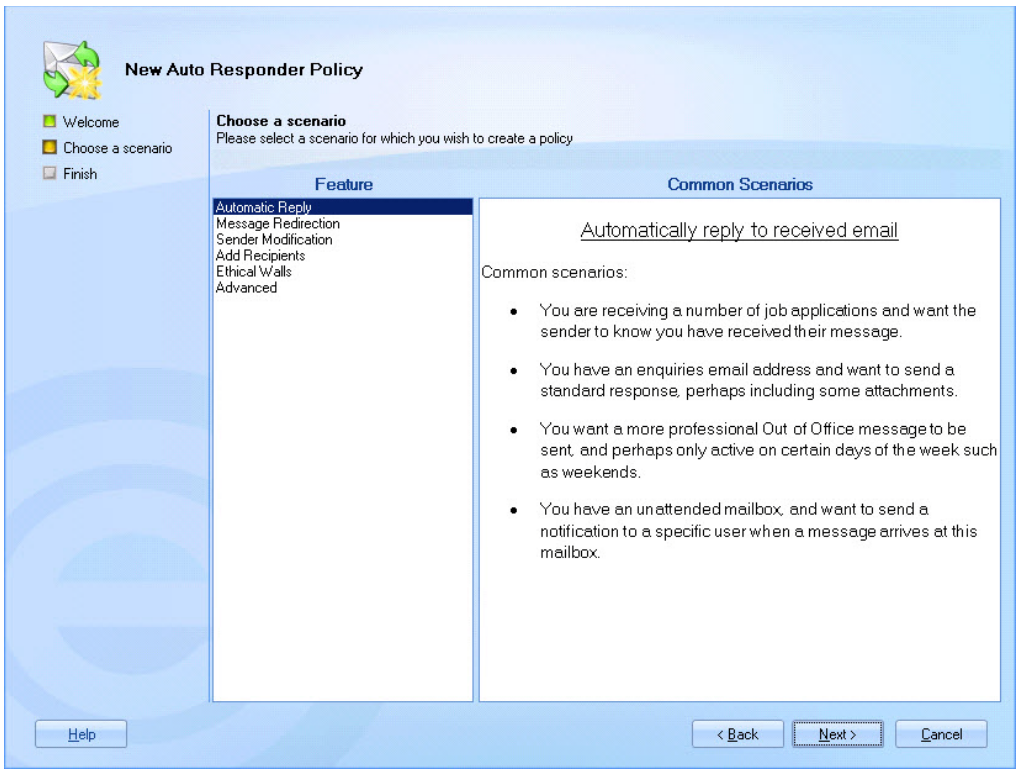
Adding an Advanced Policy

To add an advanced [see page 63] policy, follow the steps below:

1. Select the Auto Responder policies branch of the console tree.
2. Select the new policy option from the actions pane to launch the new Auto Responder policy wizard at the welcome page.

> The **new policy** option is also available using the right-click menu or from the toolbar. Alternatively, you can use the **new policy scenarios** section of the **actions** pane to select a specific policy type. If you start with a specific scenario, the **welcome** page is not displayed - go straight to step 5.

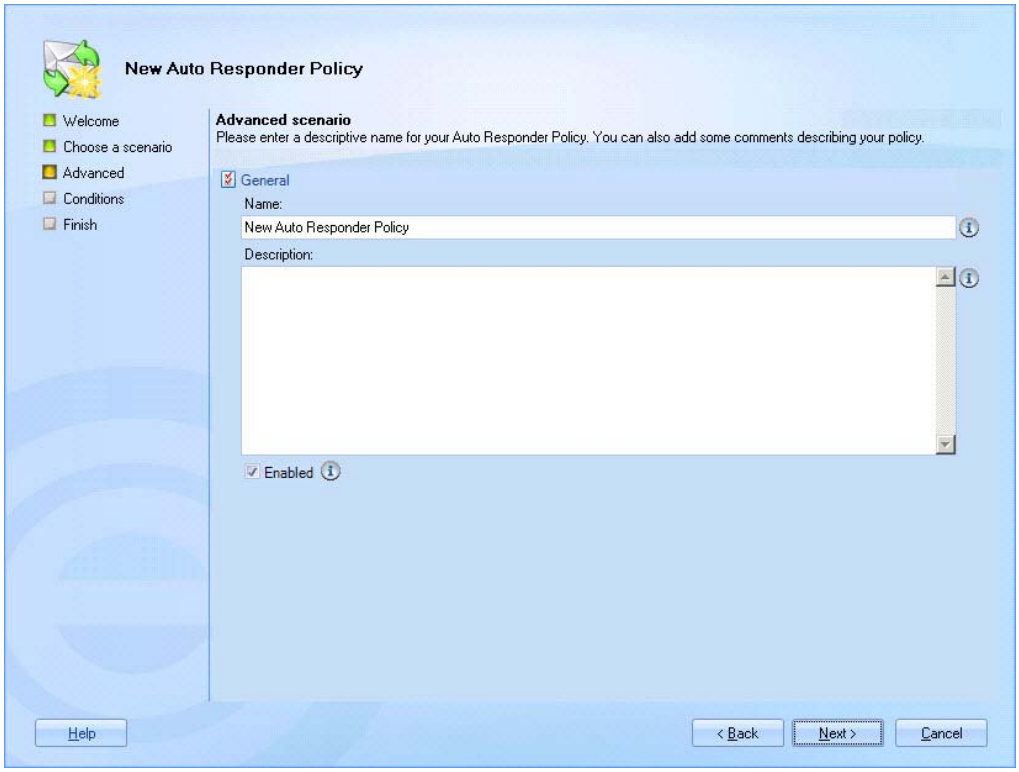
3. Click next to choose a scenario:



4. Here, available scenarios (policy types [see page 60]) are listed - if you are not sure what type of policy best suits your needs, you can select a scenario from the feature list and view summary information for each one.

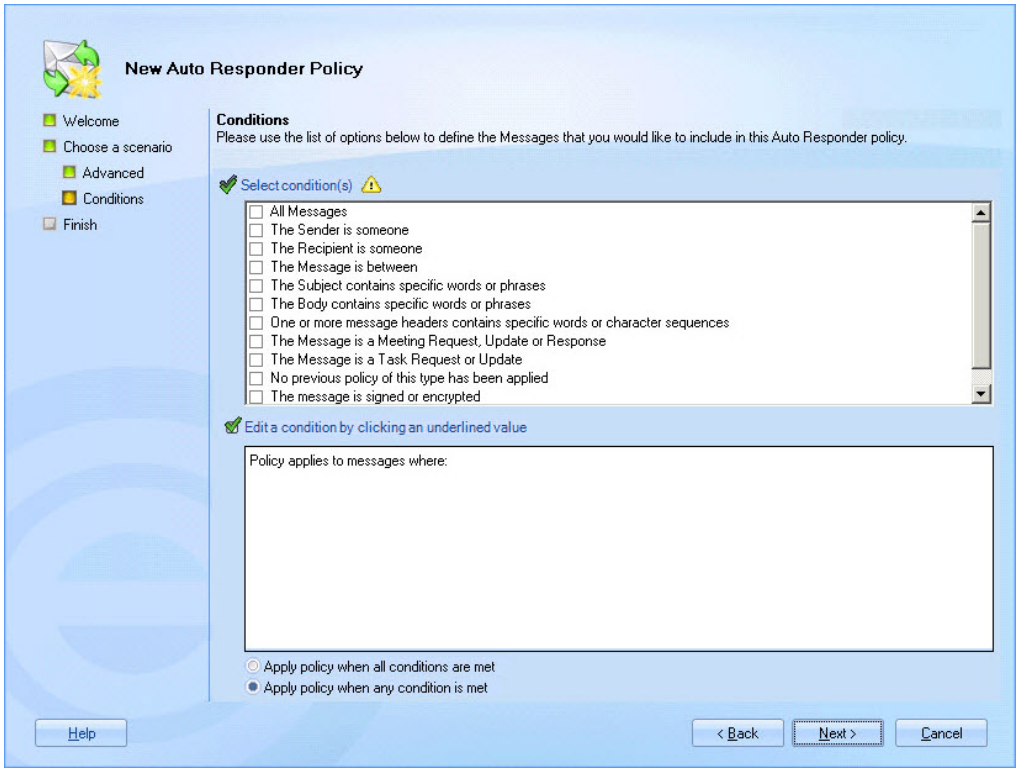
> If you started by choosing to create a specific scenario (via the actions pane), the **choose a scenario** page is not displayed - go straight to step 5.

5. Select the advanced scenario and click next to enter general information for the new policy:



6. Enter a meaningful name and description for the policy. For further information about this tab see anatomy of a policy - general on page 73.

7. Click next to view conditions:



8. Set criteria [see page 85] to determine the circumstances under which the policy is applied. Having created the policy, you can update the conditions [see page 84] at any time, and also add exceptions [see page 91] or date range [see page 96] criteria. For further information see anatomy of a policy - conditions on page 84.

9. Click next to confirm your selections and access the final page of the wizard.

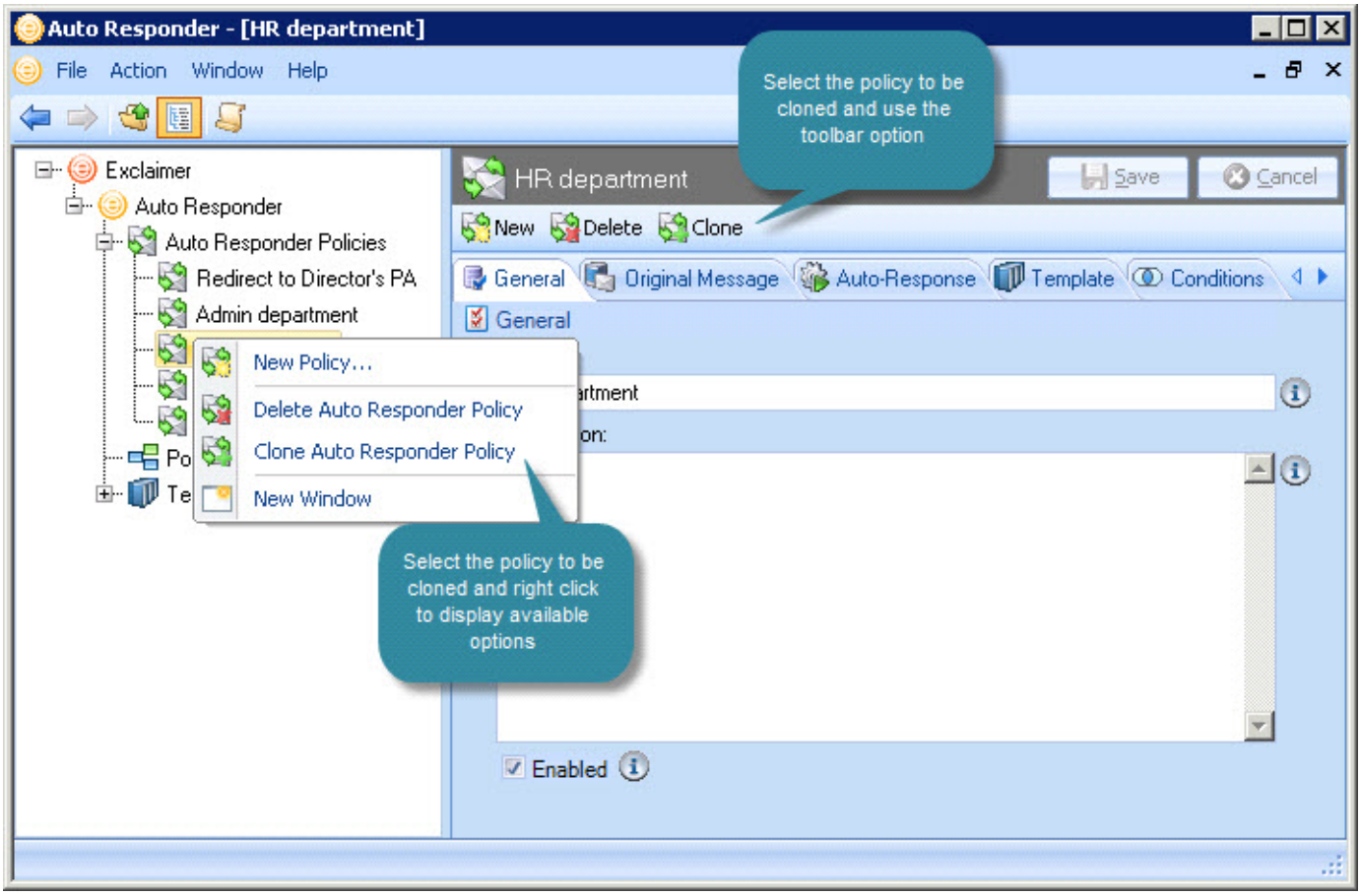
10. Click finish to complete the process and add the new policy to the policies list [see page 67].

> You must click the **save** button at the top of the Exclaimer console to save changes in Auto Responder. If you do not save changes (or if you use the **cancel** button) the new policy will not be retained when you exit from Auto Responder.

Cloning a Policy

If you need to create a new policy which has similar settings to an existing policy, it is quicker to take a copy of the existing policy and then update required settings for that copy (as opposed to creating a new policy from first principles [see page 99]).

The clone option is used to create a copy of an existing policy for this purpose, and is available from the console toolbar [see page 19], or the right-click menu:



To clone an existing policy, select the policy to be copied from the console tree, then either click the clone button from the toolbar or right click and select clone from the context menu. A copy of the selected policy is added to the console tree, ready to be updated - from here you can change the name, description and any other required settings.

When a policy is cloned, a duplicate copy of the template associated with that policy is also made and added to the template library [see page 164]. You can edit and save this template, or associate a different template [see page 132] with the new policy, as required.

Having updated the cloned policy, click save to save changes.

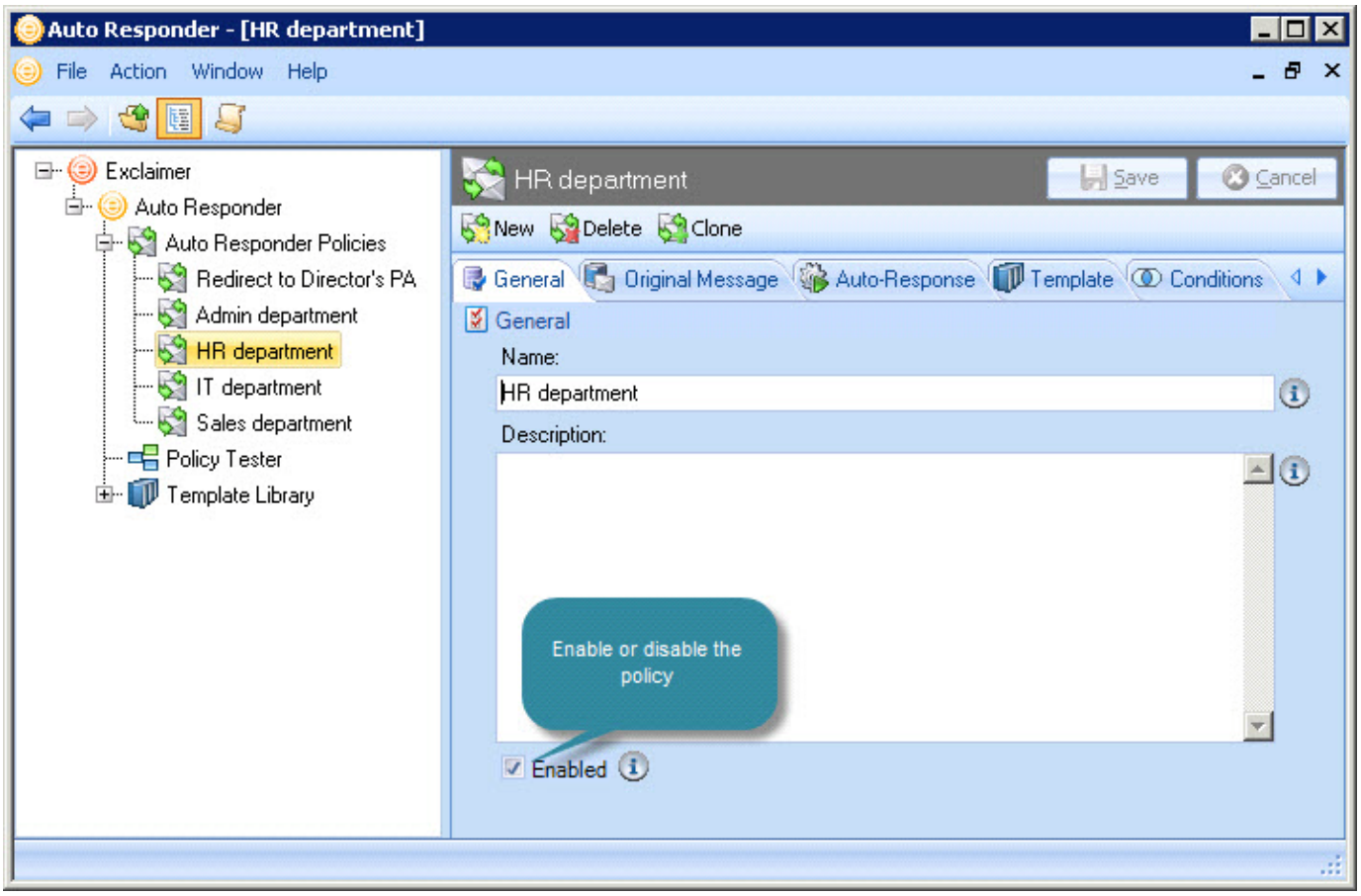
Changing a Policy

To update an existing policy, simply select the policy (either from the console tree [see page 20] or the policy list [see page 67]) and update settings on selection tabs [see page 21] as required.

When a policy has been changed but not saved, the branch is displayed with an asterisk (*) symbol. You can see which tabs contain these unsaved changes, by looking for an asterisk to the right of the tab name. When you are satisfied that all required changes have been made correctly, click save to save the new settings. All asterisk symbols are cleared once changes have been saved.

Enabling and Disabling a Policy

A policy must be enabled in order for it to be processed. When a new policy [see page 99] is added, it is enabled by default; however there may be times where you need to change this setting. To quickly enable or disable a policy, select the required policy (either from the console tree [see page 20] or the policy list [see page 67]):

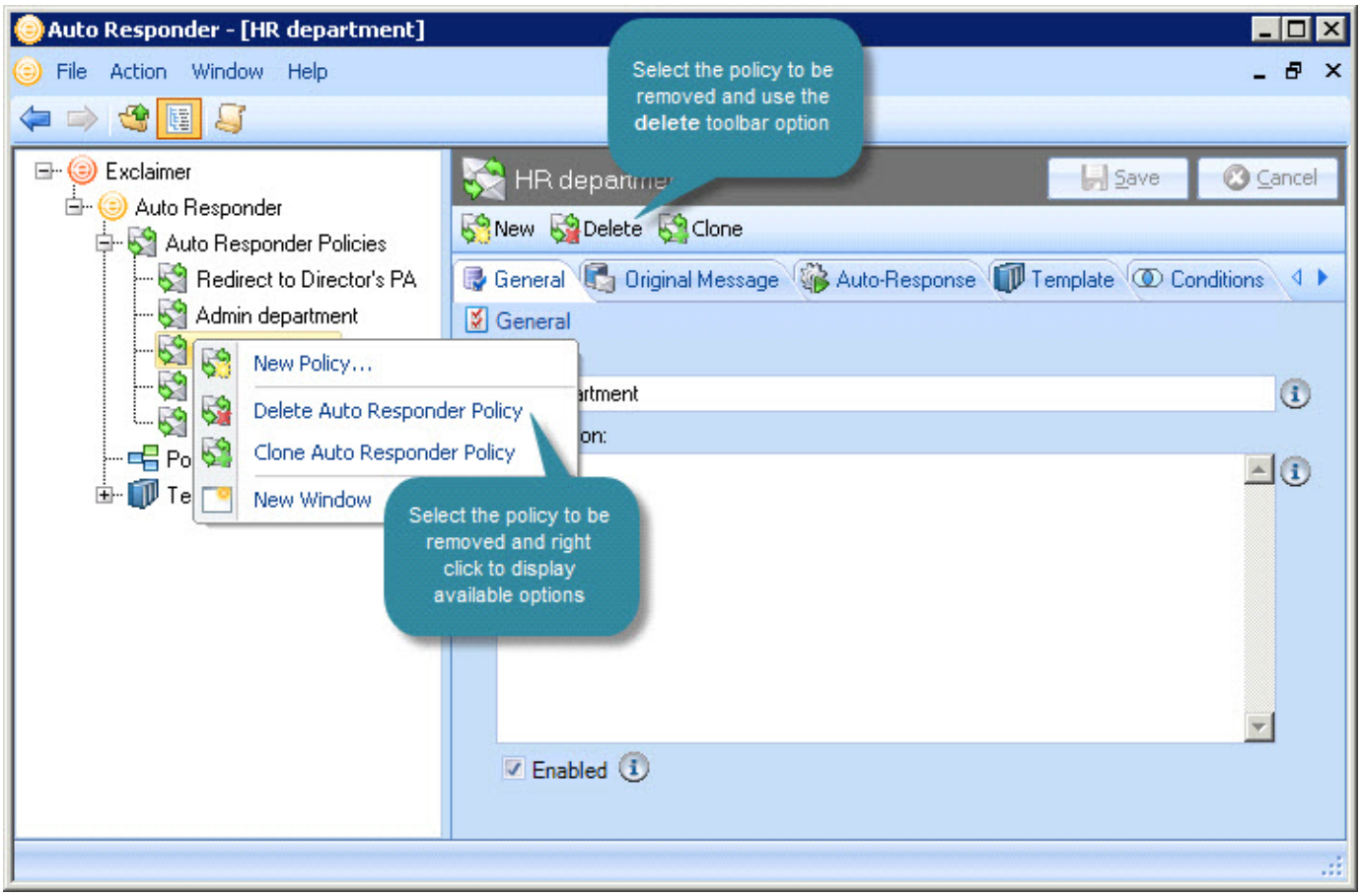


Ensure that the enabled check box is selected to enable the policy, or de-selected to disable the policy. Click save to save changes.

If you do not save changes, any enable/disable changes will not be applied.

Removing a Policy

To remove an existing policy, select the policy (either from the console tree [see page 20] or the policy list [see page 67]). Then, either right click and select delete from the context menu, or click the delete button on the toolbar:



Having chosen to delete a policy, you are asked are you sure you want to delete this policy?.

Click yes to confirm the deletion or no to abandon the task. Finally, click save to save changes.

> A policy is not permanently deleted until settings have been saved. If you exit without saving (or if you **cancel** changes), the policy will be reinstated in the console tree.

How To...

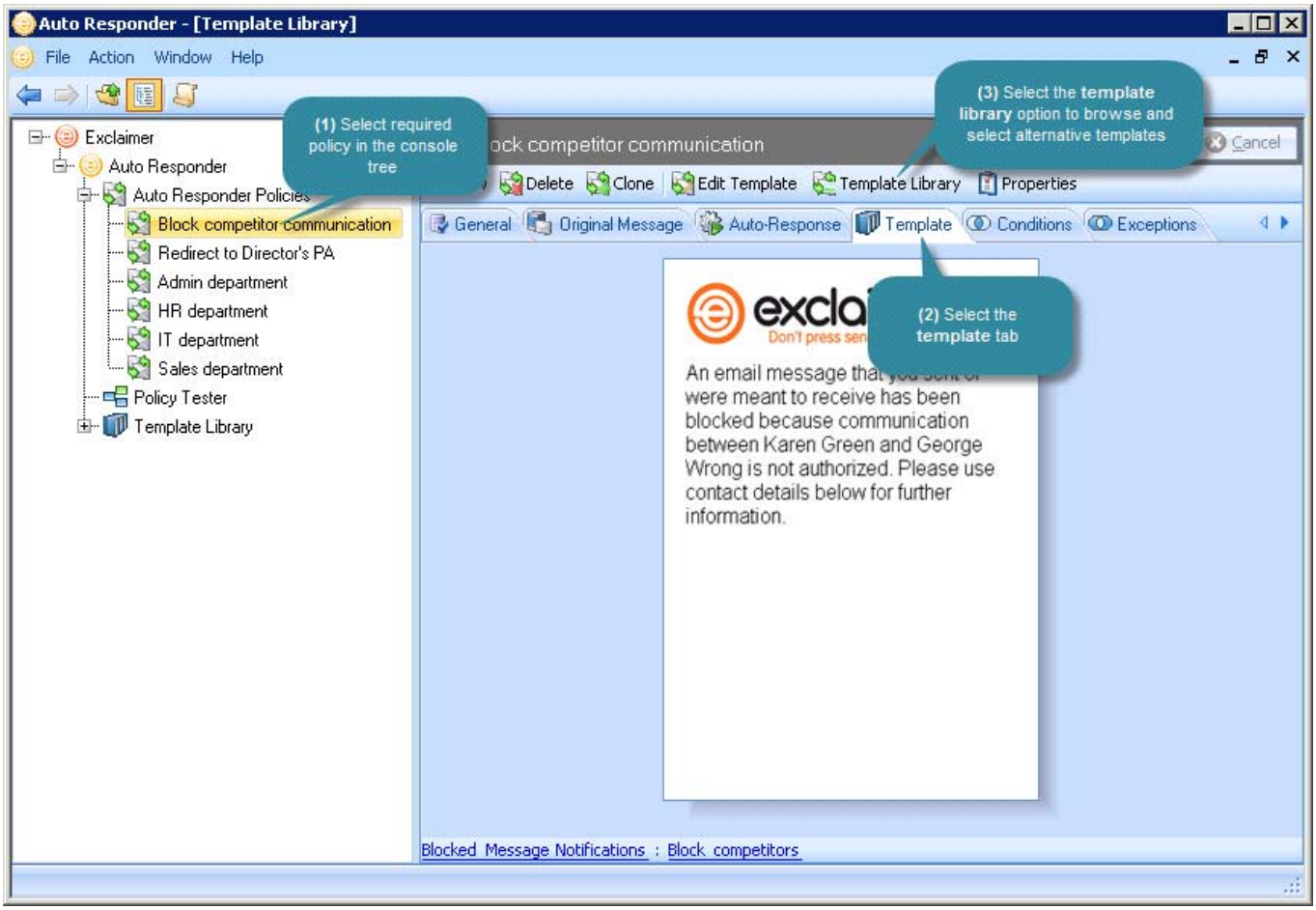
This section contains instructions for completing a selection of common tasks with policies using Exclaimer Auto Responder, including:

- How do I change the template associated with a policy? [see page 132]
- How do I change the sequence in which polices run? [see page 134]
- How do I create a policy based on specific Active Directory attributes? [see page 135]
- How do I block emails between two email accounts? [see page 142]
- How do I define a policy based on a subject line trigger word? [see page 144]
- How do I create a policy for all internal or all external emails [see page 147]
- How do I send file attachments with an automatic reply? [see page 149]
- How do I implement an out of office reply? [see page 150]

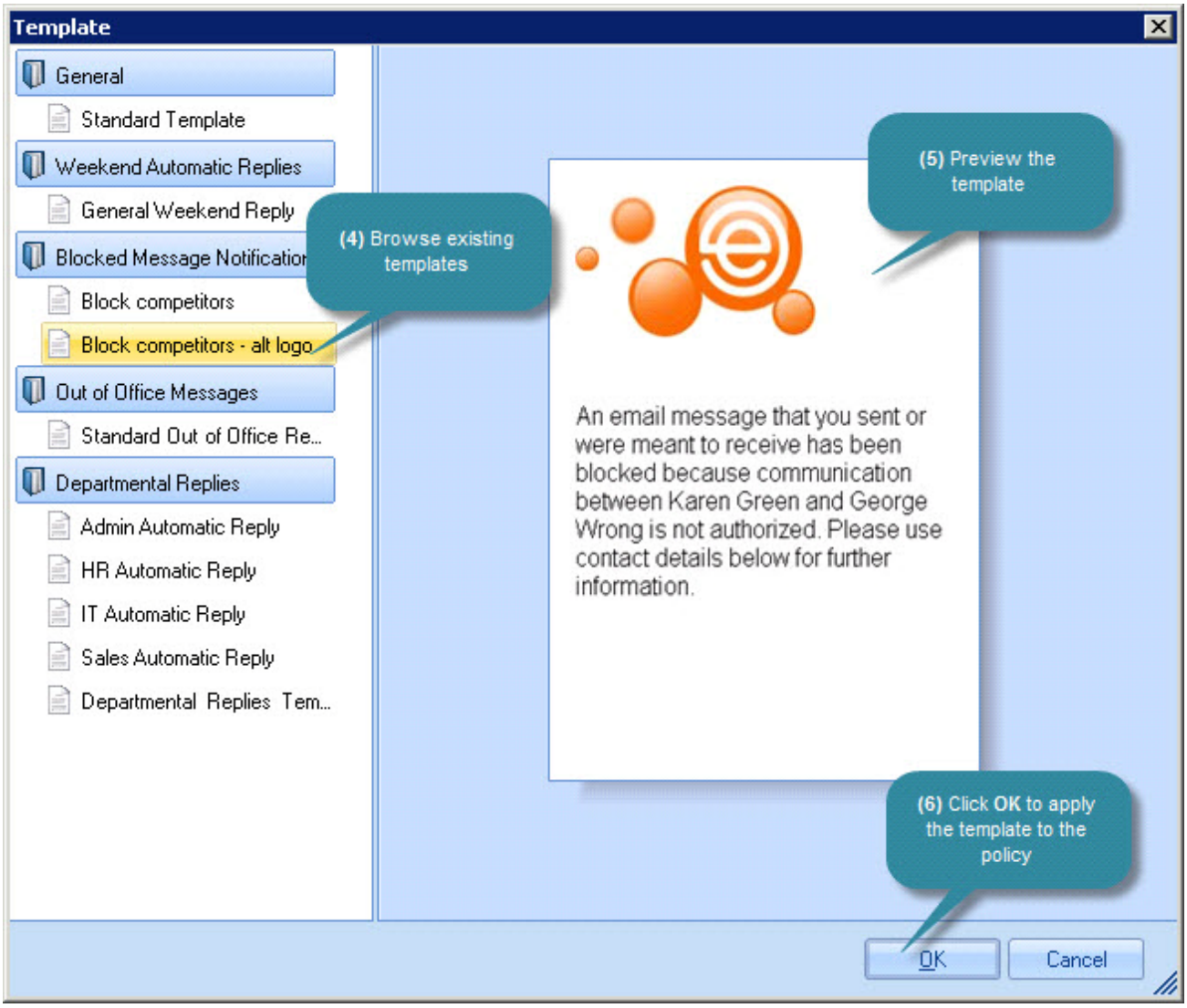
How do I Change the Template Associated with a Policy?

When viewing the template associated with a policy, you can choose to access the template library [see page 164] and select a new template, as shown below.

Steps 1 - 3: Access the Template Library from Within a Policy

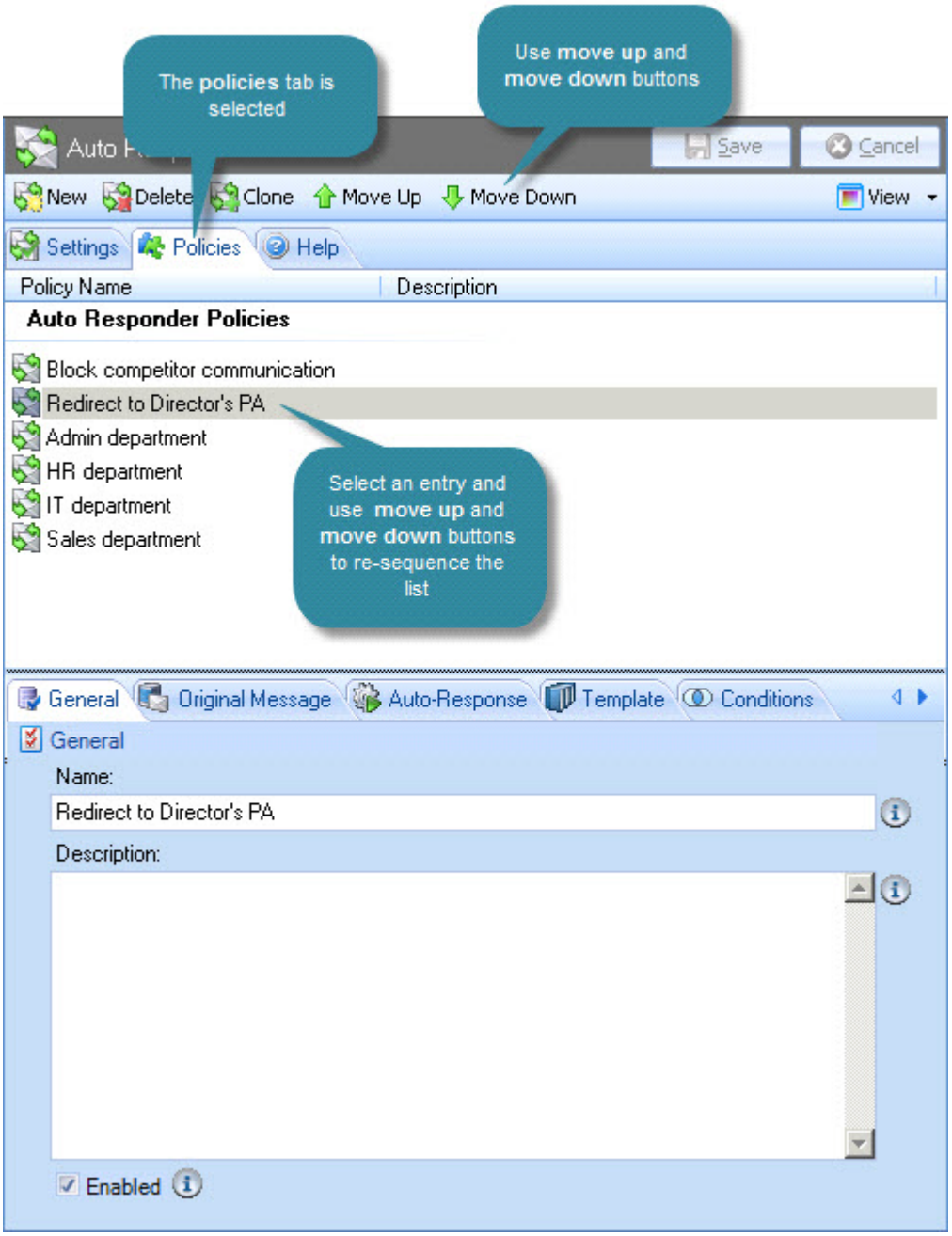


Steps 4 - 6: Browse and Select New Templates



How do I Change the Sequence in which Polices Run?

Policies are processed in the order that they are listed in the policies tab [see page 67] (this sequence is also reflected in the console tree [see page 20]). To change the sequence in which policies are listed, access the policies tab and use move up / move down buttons as required:

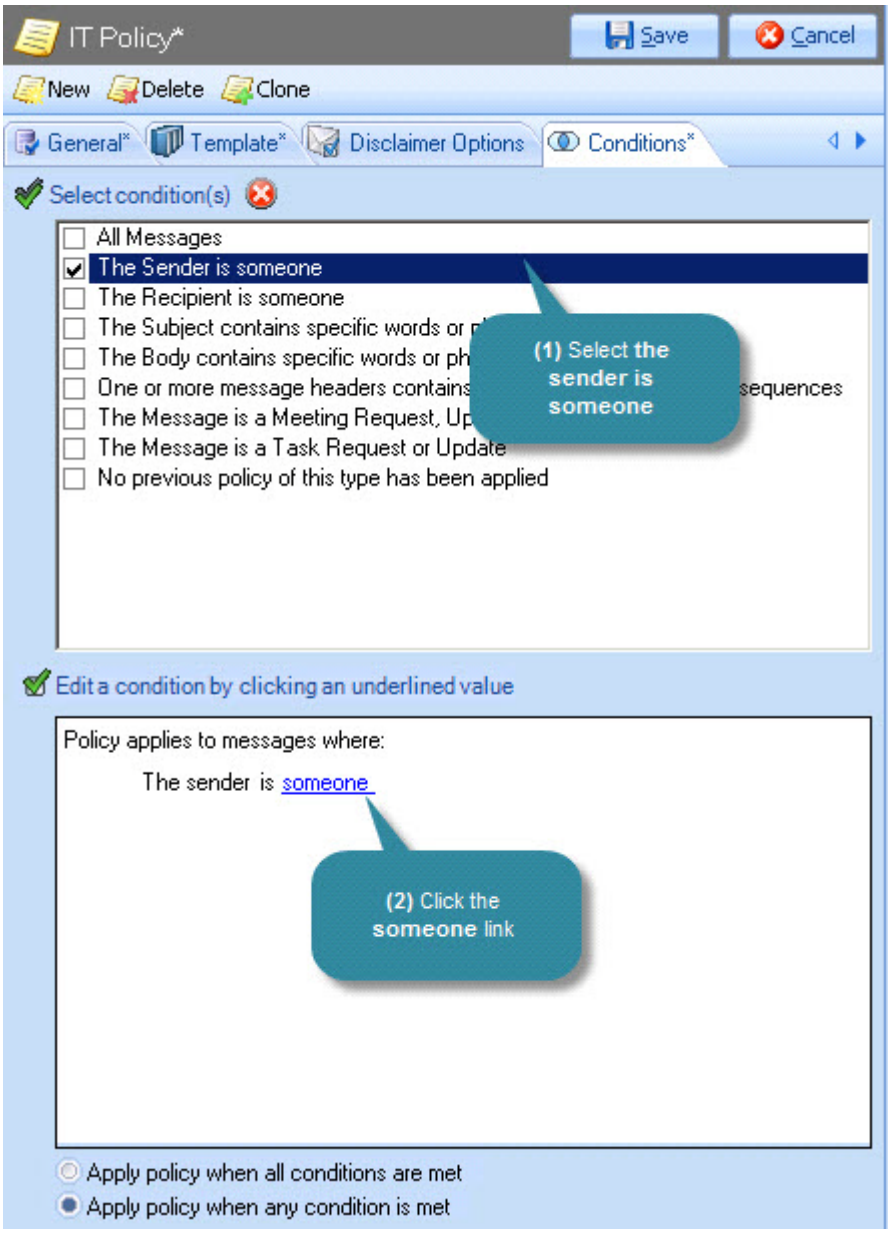


How do I Create a Policy Based upon Specific Active Directory Attributes?

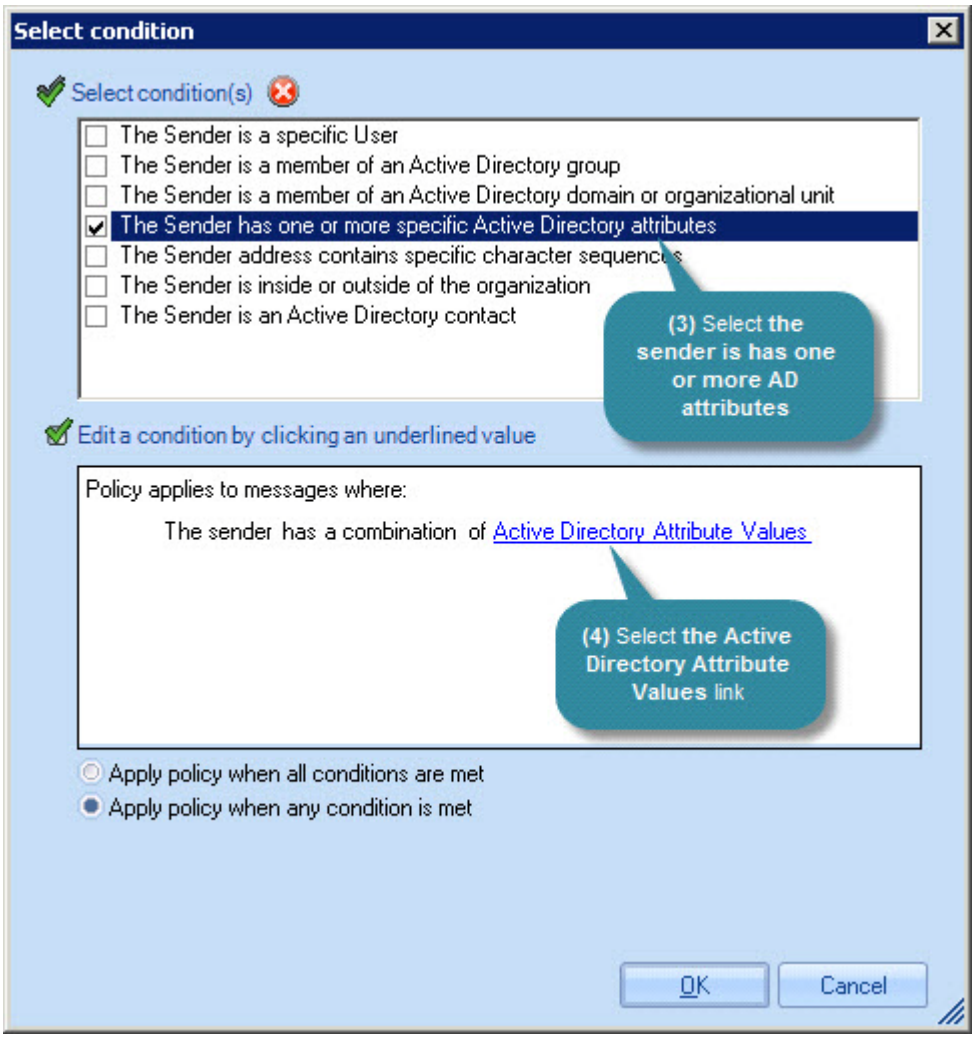
The configure attributes window [see page 89] allows you to define conditions [see page 84] and exceptions [see page 91] based upon queries that are run on Active Directory user attributes.

The following example shows how to set a policy condition which uses an Active Directory attribute query. In this scenario, a policy is required to apply an auto response for everyone within the 'IT' department of an organization.

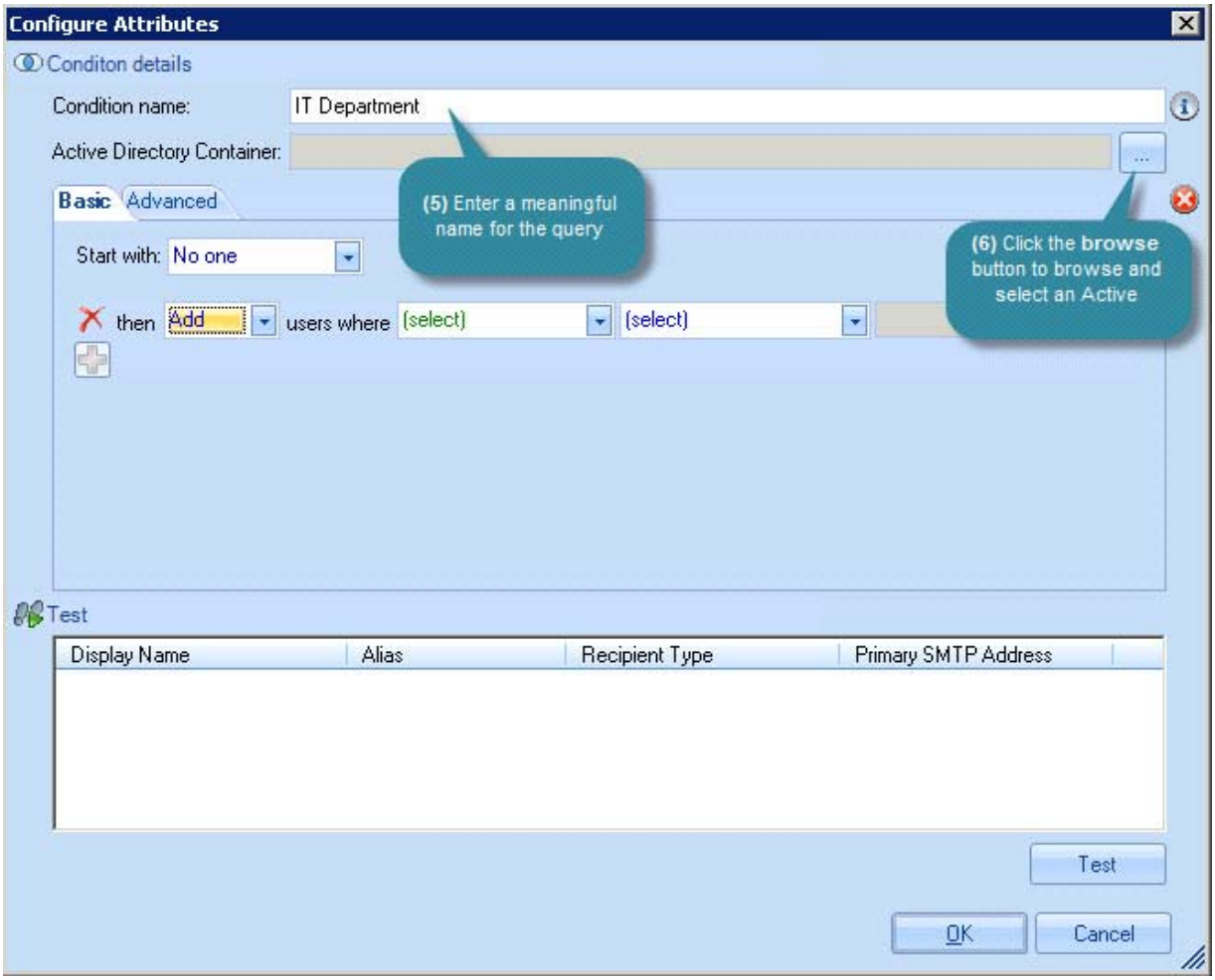
Steps 1 and 2: 'The Sender is Someone'



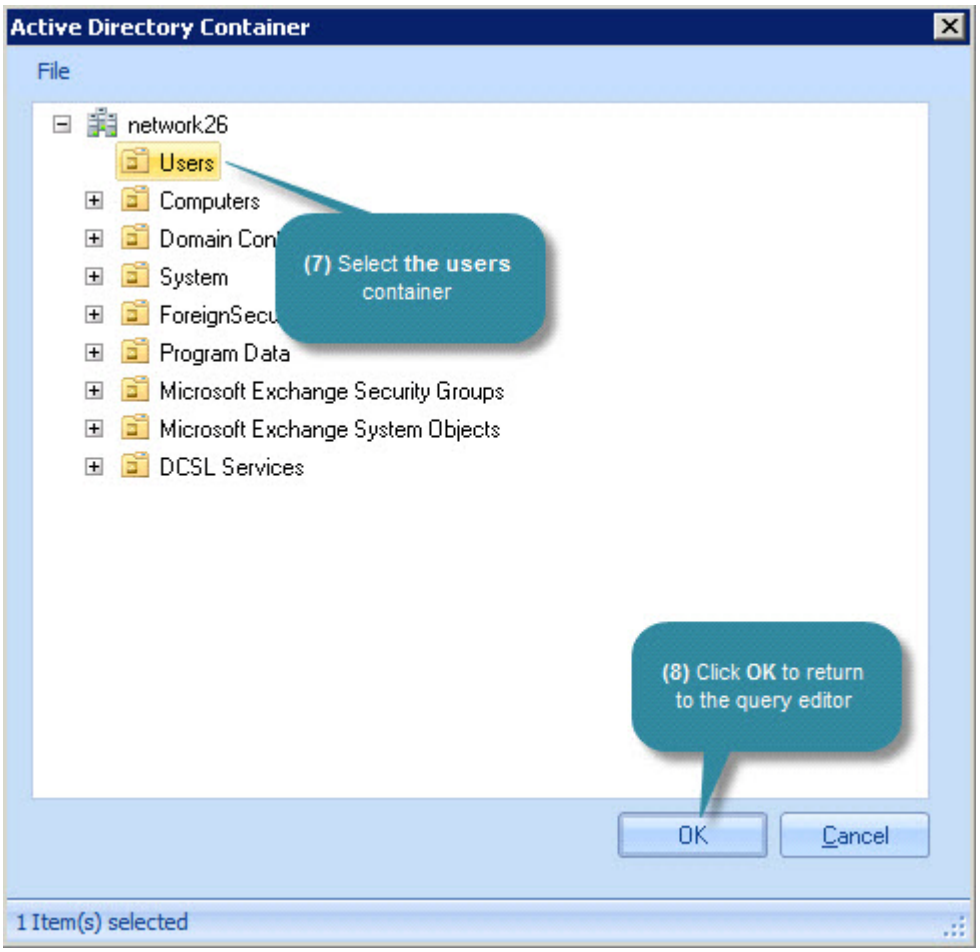
Steps 3 and 4: 'The Sender has One or More Specific AD Attributes'



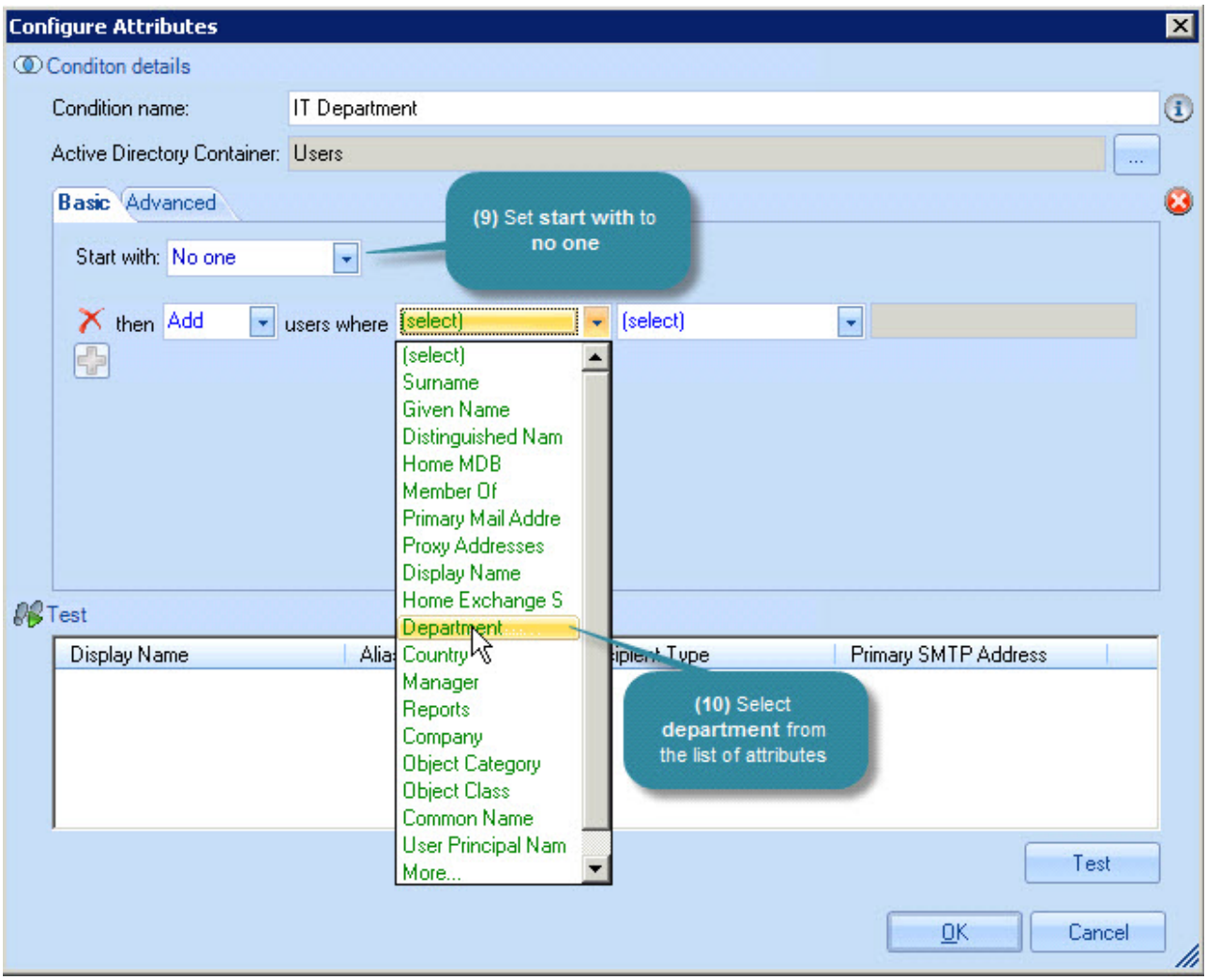
Steps 5 and 6: Enter Basic Details for the Query



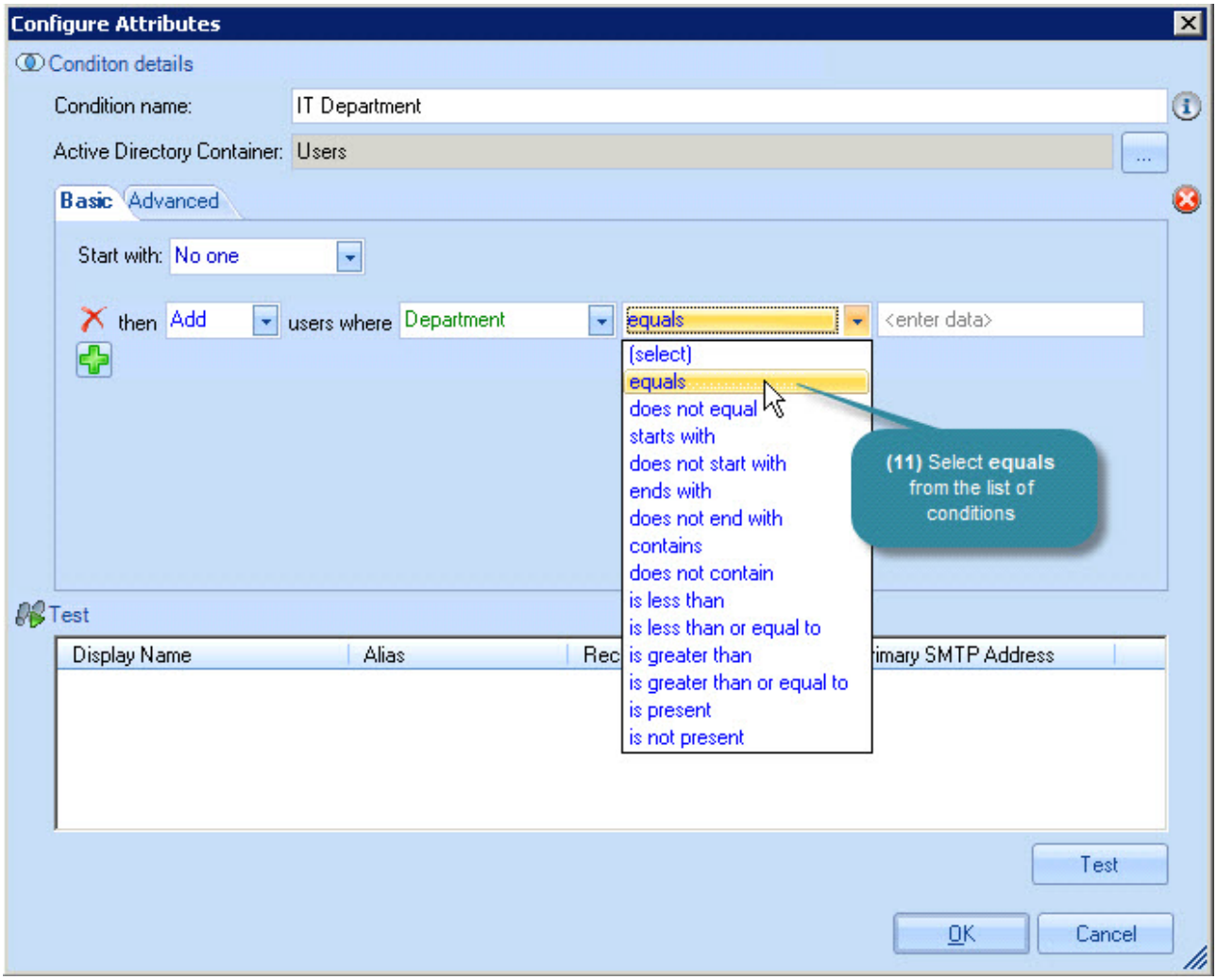
Steps 7 and 8: Browse and Select an Active Directory Container



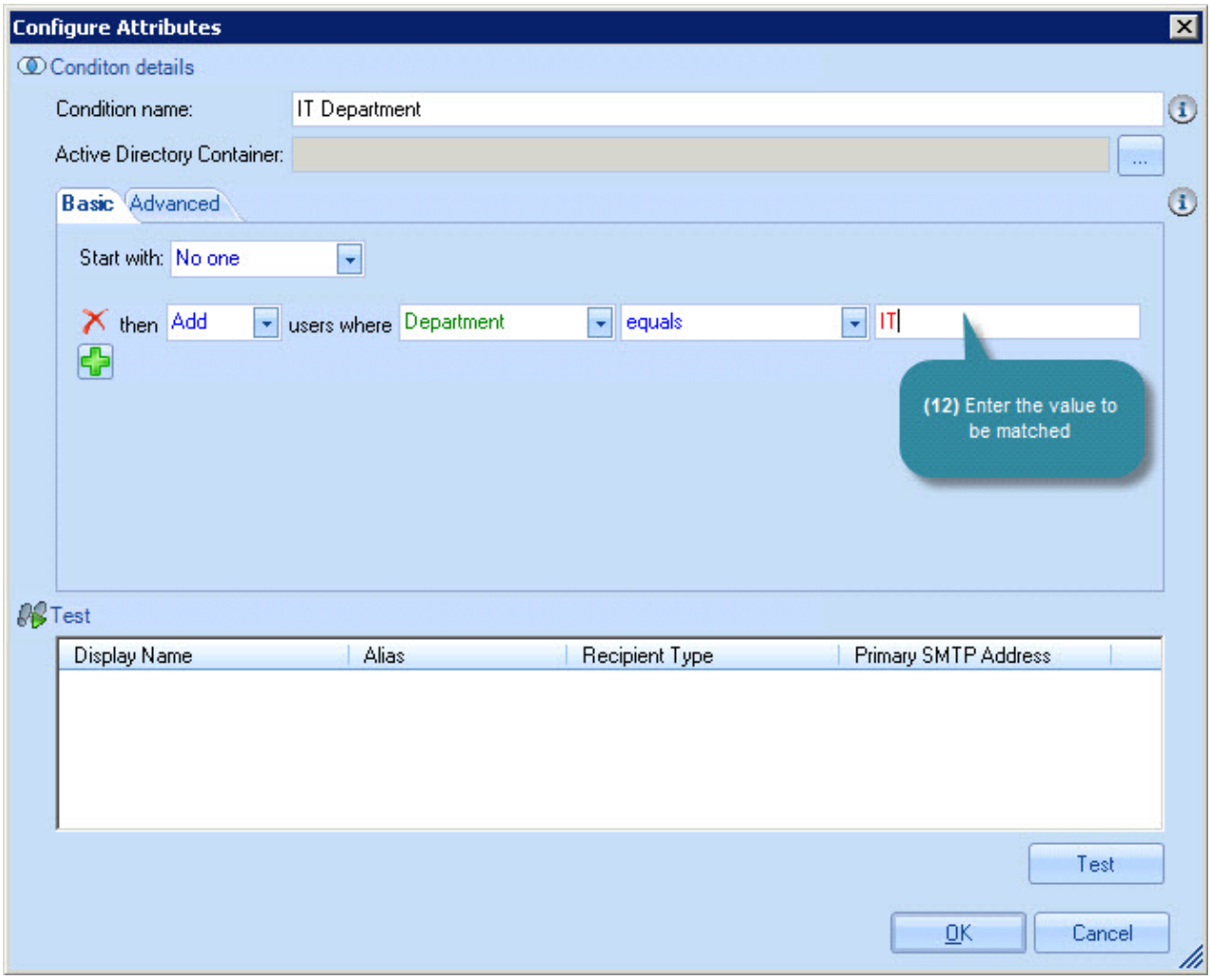
Steps 9 and 10: Choose a Start Point and Select Required Attribute



Step 11: Choose how Matching Should be Made



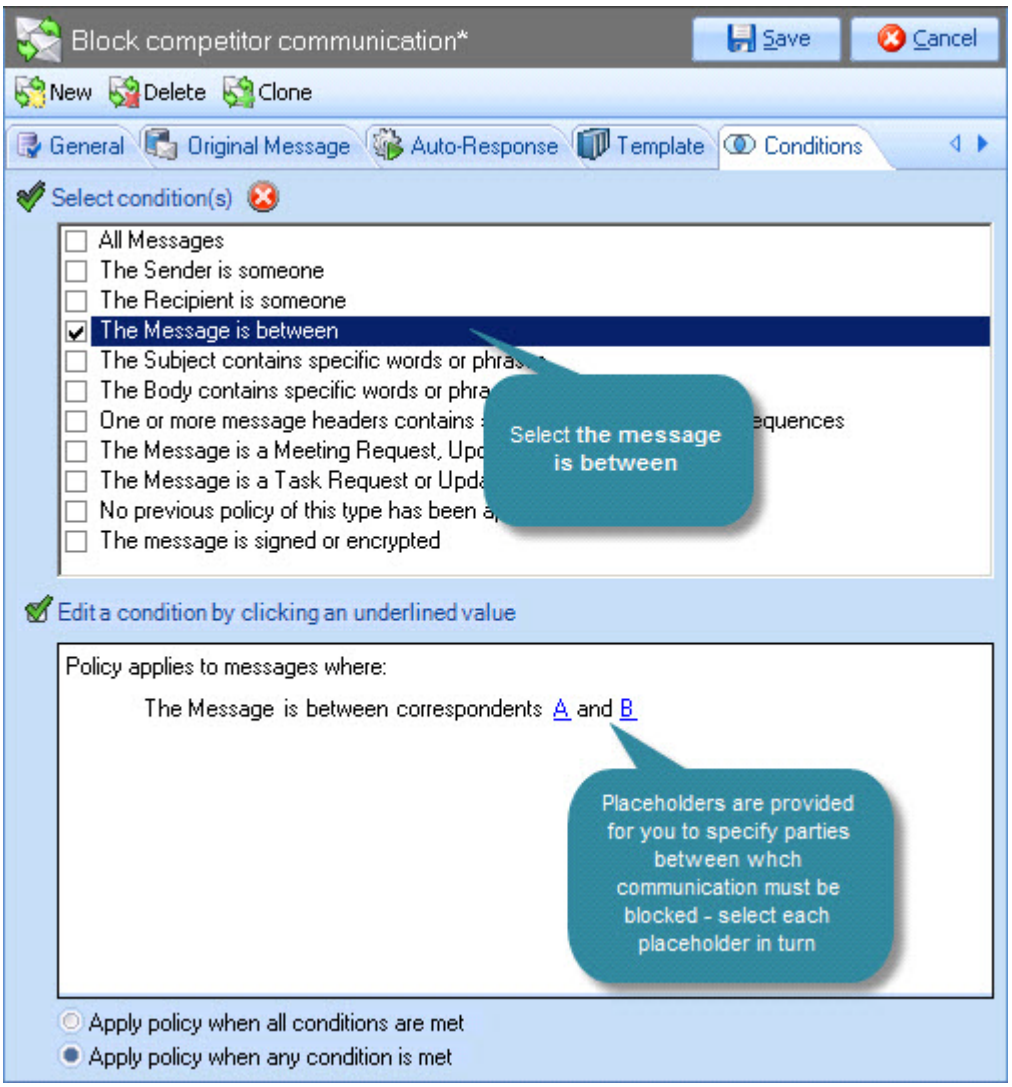
Step 12: Enter the Required Attribute Value for Matching



How do I Block Emails between Two Parties?

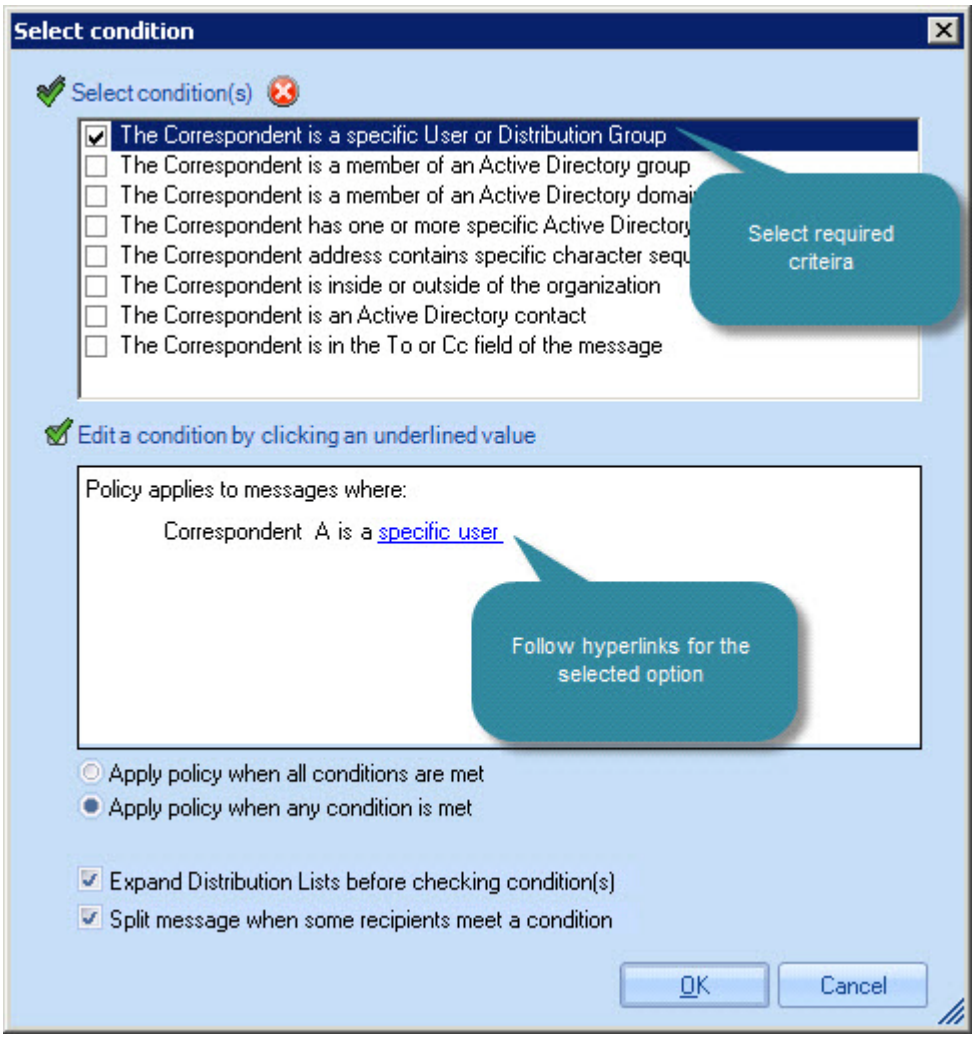
There may be times where the appropriate automated response for a given situation is to block emails between two parties - for example, where a conflict of interest may arise. The best way to do this to create an ethical walls policy [see page 62].

This type of policy uses a condition [see page 84] called the message is between. When this condition is selected, you can choose two parties between which email communication should be blocked:



Placeholders are provided for A and B. These need to be selected and replaced with criteria to define the two parties between which emails should be blocked.

Having selected a placeholder for the condition, you can specify further criteria:



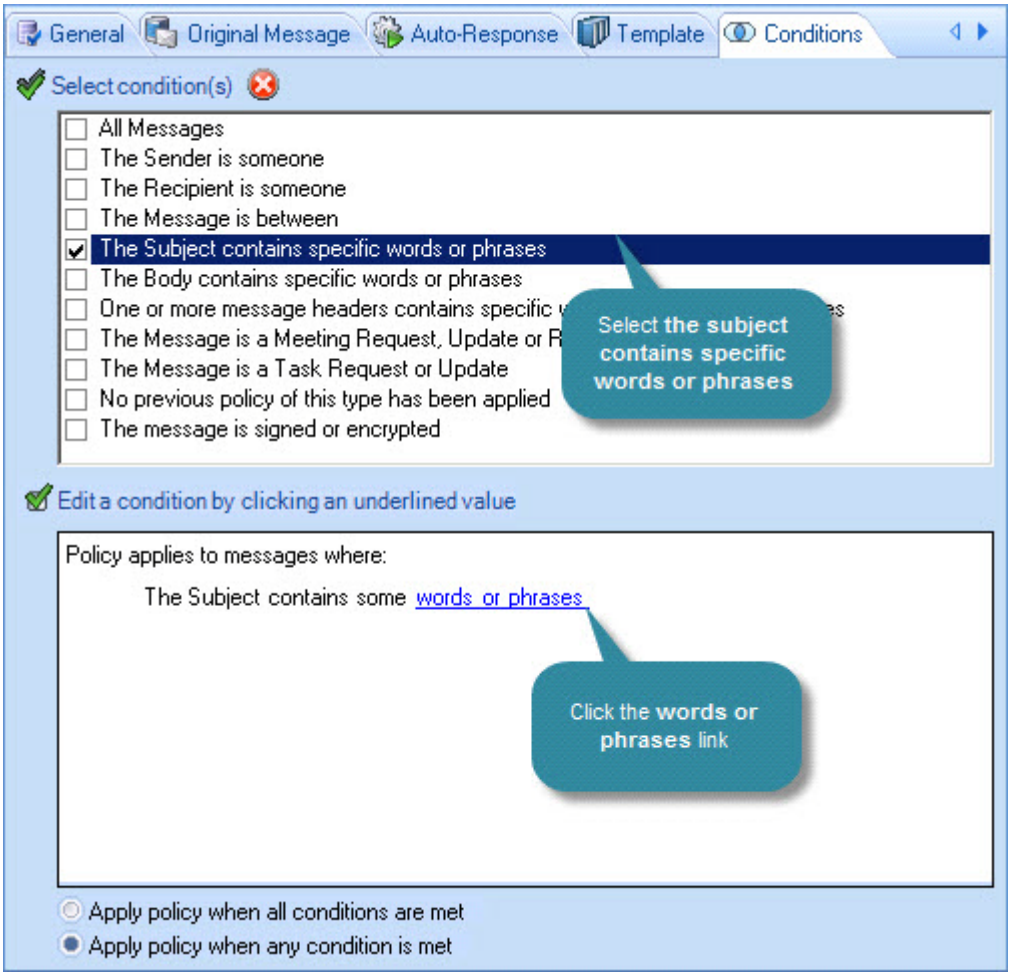
How do I Define a Policy Based upon a Subject Line Trigger Word?

It is sometimes useful to apply an automated response based upon a 'trigger word' in the subject line of emails. For example, you might wish to create a message redirection policy [see page 61] where emails which include a given word in the subject should be redirected to an alternative address.

To achieve this, you should define a policy where the conditions [see page 84] are set for subject contains specific words or phrases, as shown below:

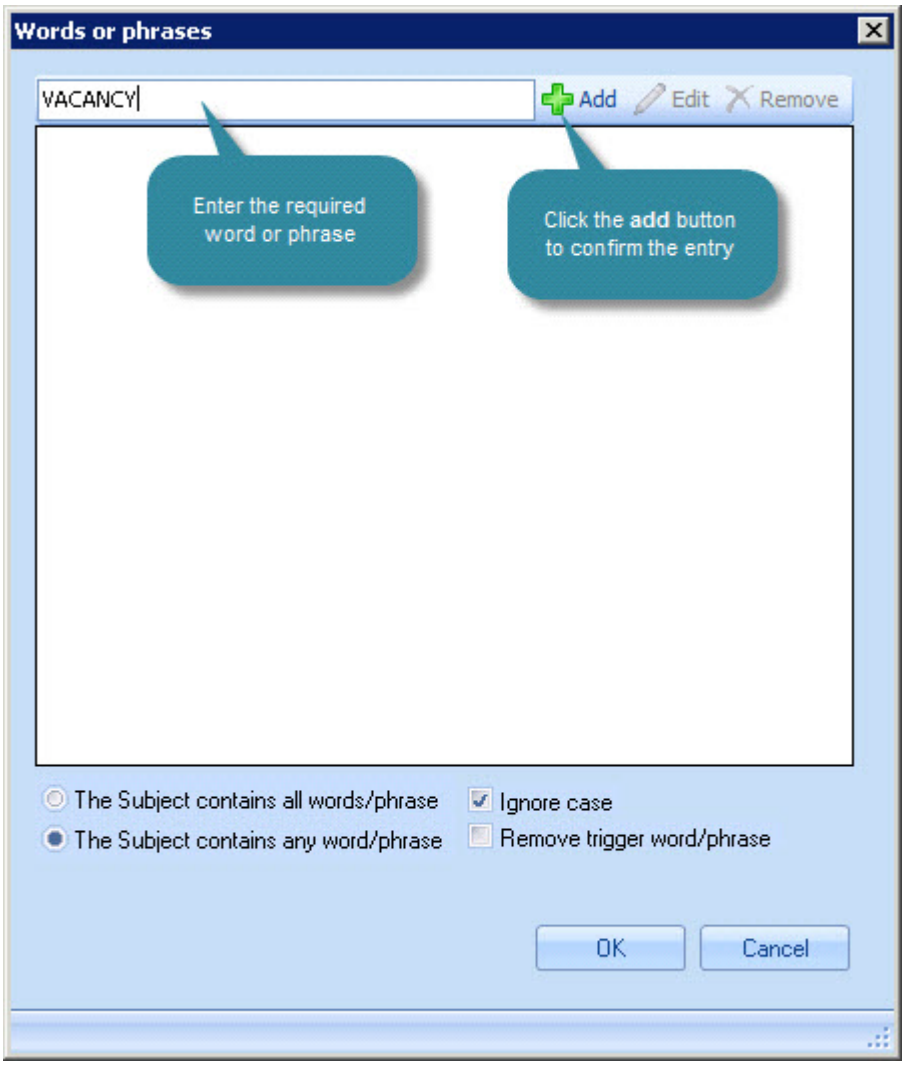
Step 1: Select 'The Subject Contains Specific Words or Phrases' Option

Having selected this option, click the words or phrases link in the lower pane:



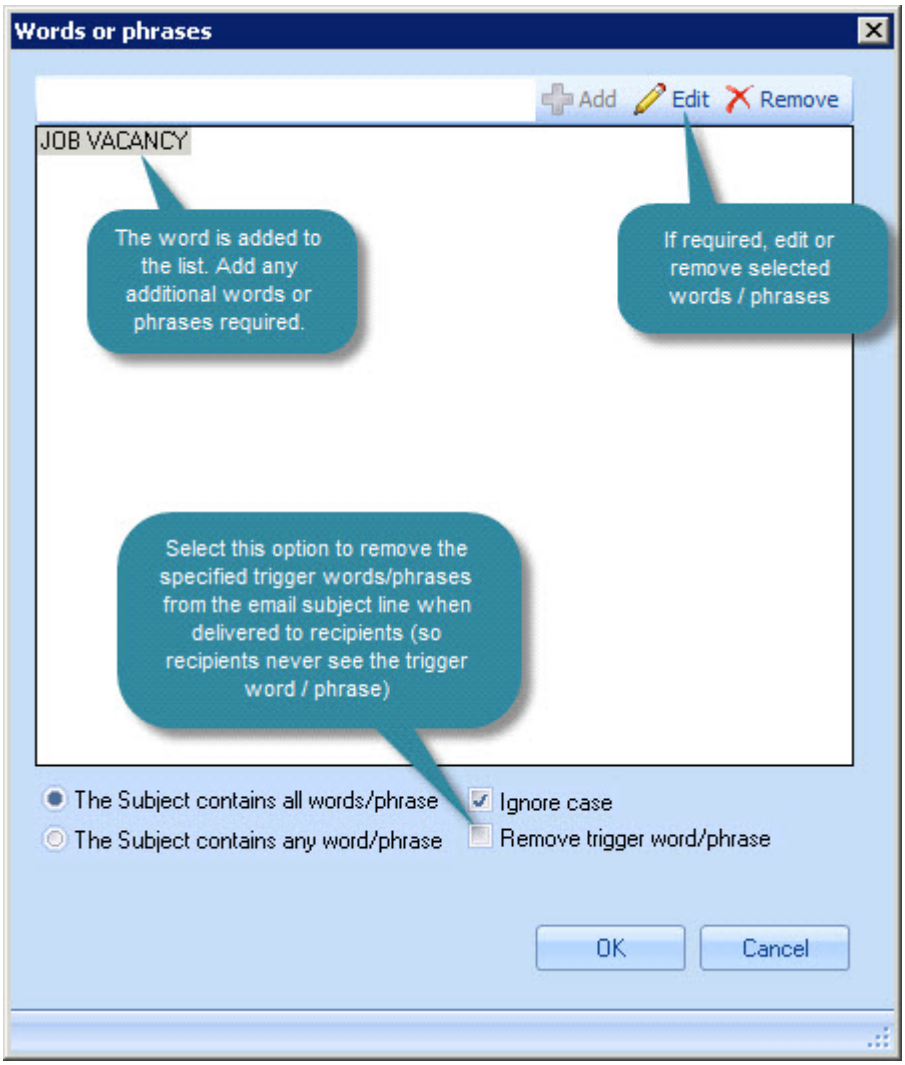
Step 2: Add Required Words and Phrases

Enter as many words and phrases as required, using the add button to confirm each one. If you specify multiple words in a single line, they are treated as a phrase:



Step 3: Set Options for Words and Phrases

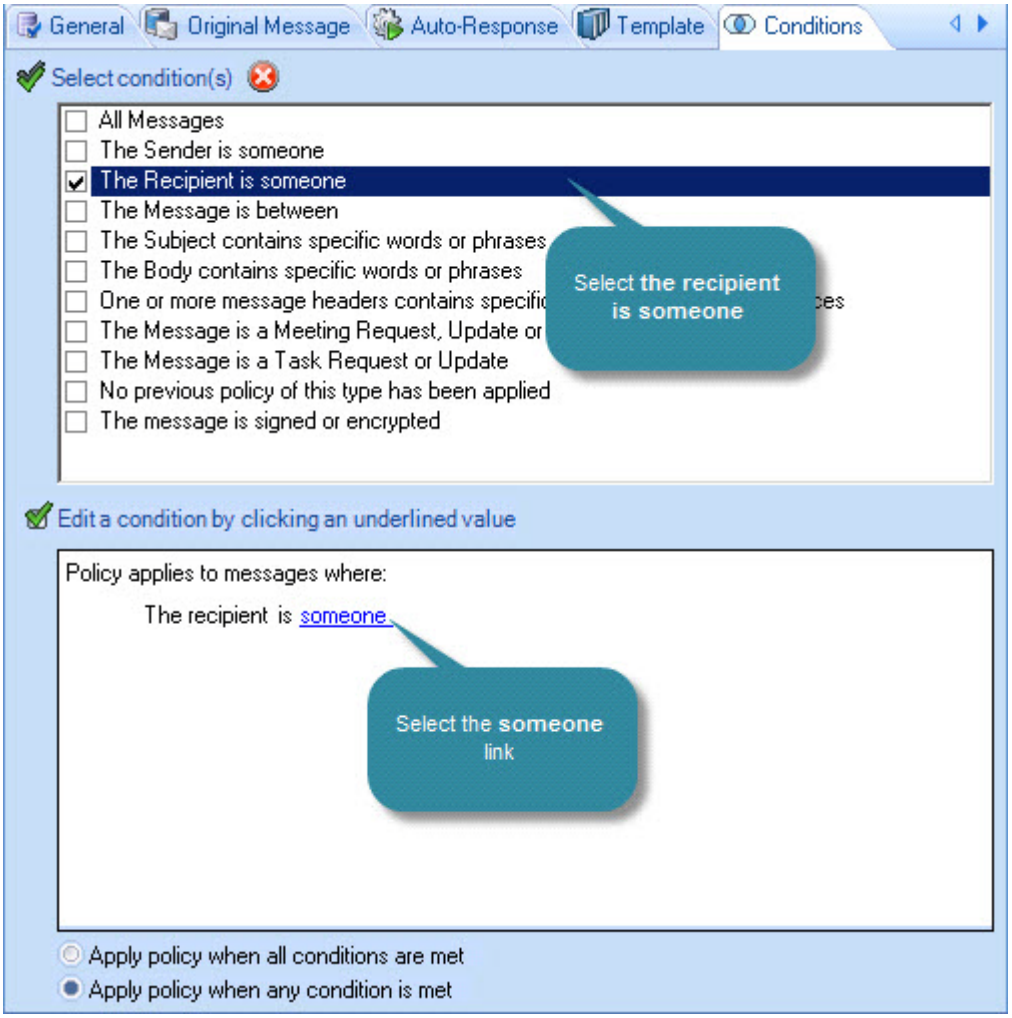
Choose whether all or any words / phrases must be present to trigger the policy. Also choose whether or not to ignore case, and whether or not to remove trigger words / phrases:



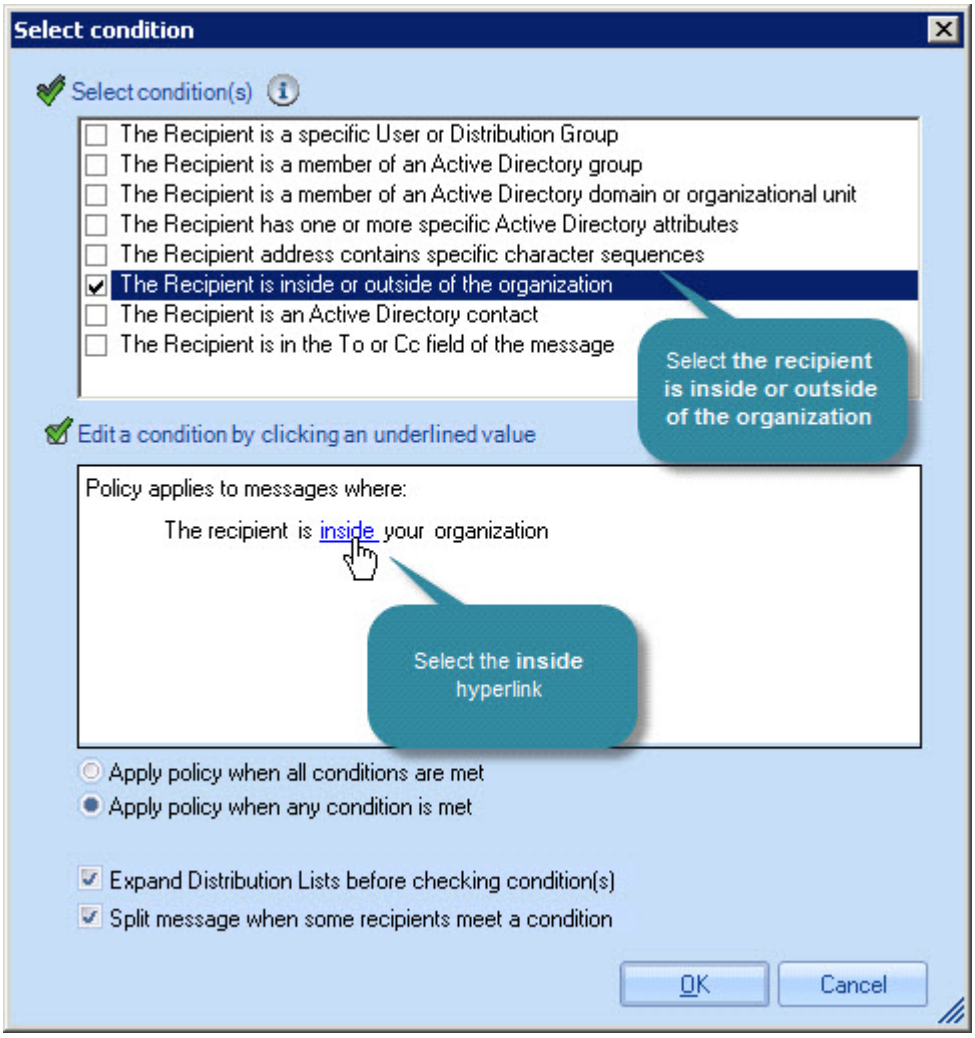
How do I Create a Policy for All Internal or All External Emails?

In some cases, you may wish to apply a policy for only internal or only external emails. This can be done using conditions [see page 84], as shown below:

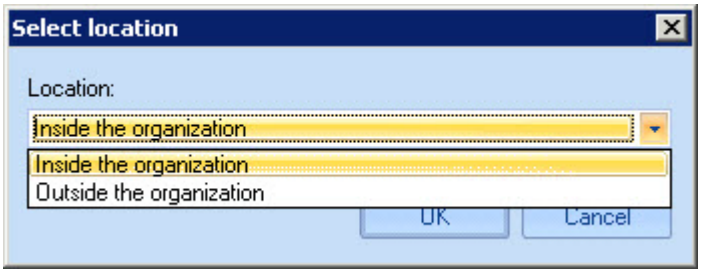
Step 1: Access Policy Conditions and Select 'The Recipient Is Someone'



Step 2: Click the 'Someone' Link in the Lower Pane



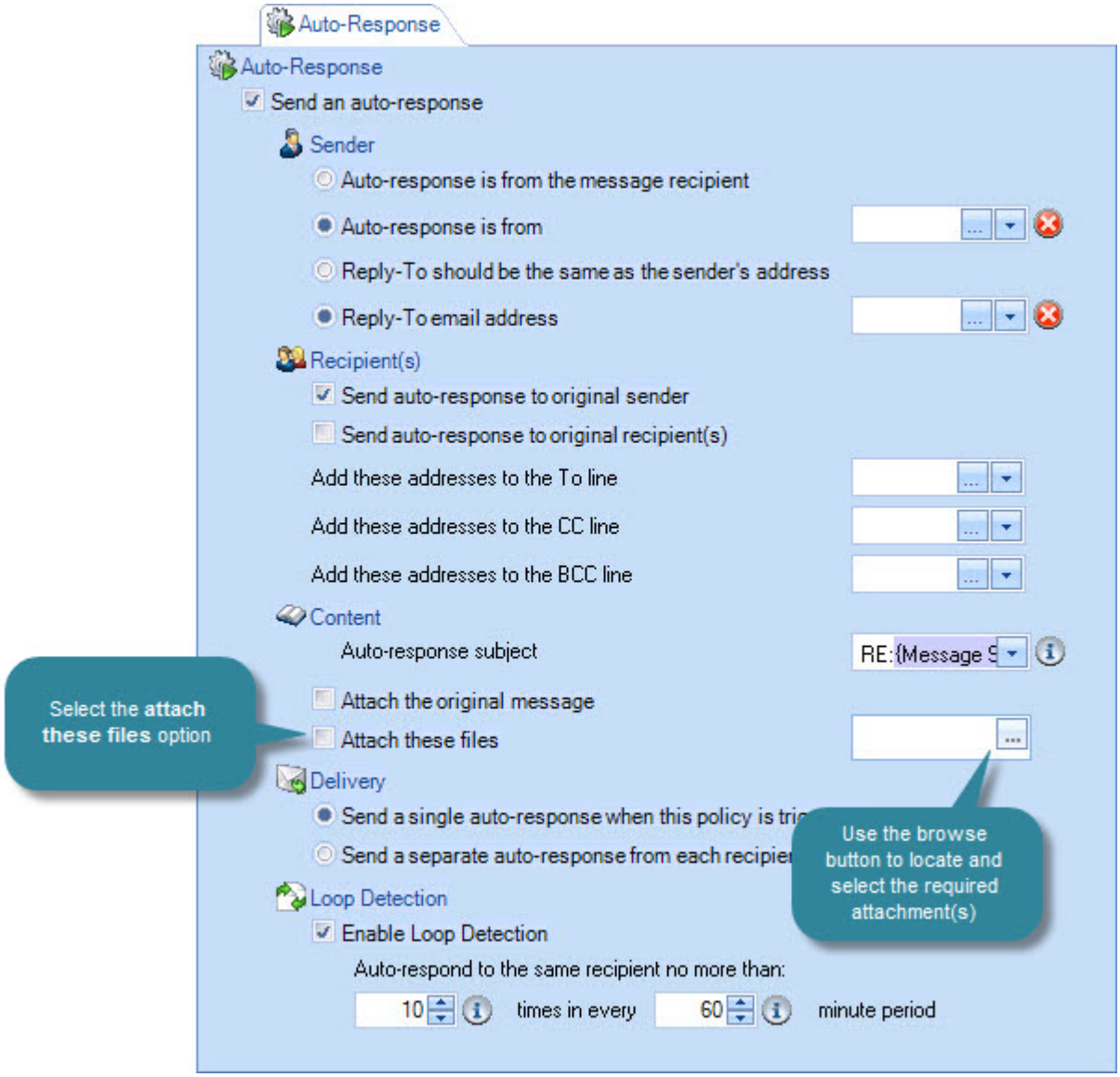
Step 3: Select 'Recipient is Inside or Outside of the Organization'



How can I Send File Attachments with an Automatic Reply?

There may be times where it is useful to send file attachments with an automatic reply. For example, you might create a policy to send an automatic reply to emails concerning an advertised job vacancy, and wish to send company literature with the automated reply.

To send attachments in this way, simply select the attach these files option on the auto response tab [see page 78] for the policy:

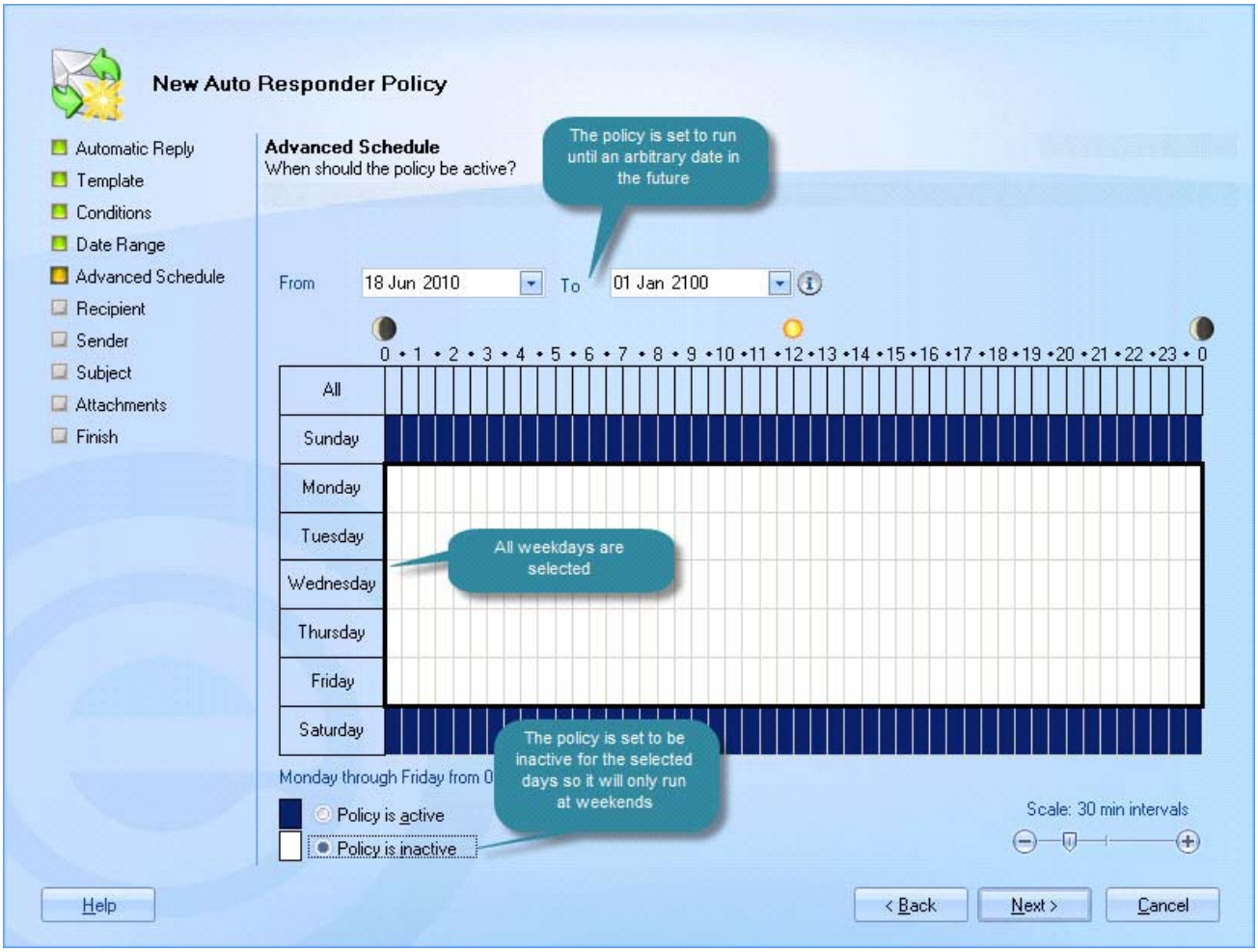


Having chosen to attach these files you should use the browse button to open the insert file attachments window. From here you can navigate local and network drives to select the required file attachment. If required, you can select multiple attachments.

How do I Implement an Out of Office Reply?

To create an automated Out of Office reply, you would need to create a template [see page 164] which contains required content for the reply, and define an automatic reply policy [see page 60].

When defining the automatic reply policy, you should set conditions [see page 84] and exceptions [see page 91] to determine the circumstances under which the Out of Office reply will be sent. For example, you might define a policy that is triggered for all Active Directory contacts with exceptions for a technical support group. To trigger the policy only at weekends, you would use the advanced schedule from the date range [see page 96] tab:



It is important to note that Exclaimer Auto Responder does not affect any Out of Office settings that users may set locally, using Microsoft Outlook.

If you define an Auto Responder policy to send an Out of Office reply for a given user and that user has set their own Out of Office reply using Microsoft Outlook, the recipient would receive both replies.

If you are using Auto Responder to manage Out of Office replies, you should advise users not to define local Out of Office settings in Outlook.

Chapter 5

The Policy Tester

Introduction

The policy tester is used to create a test email and simulate the sending process, so you can ensure that automatic responses are applied correctly.

Messages generated in the policy tester are never actually sent so you can select whichever sender and recipient is most appropriate for testing a policy, without concern. Using the policy tester, you can:

- Define a test message [see page 156]
- Save a test message for later use [see page 157]
- Load a saved message for testing [see page 157]

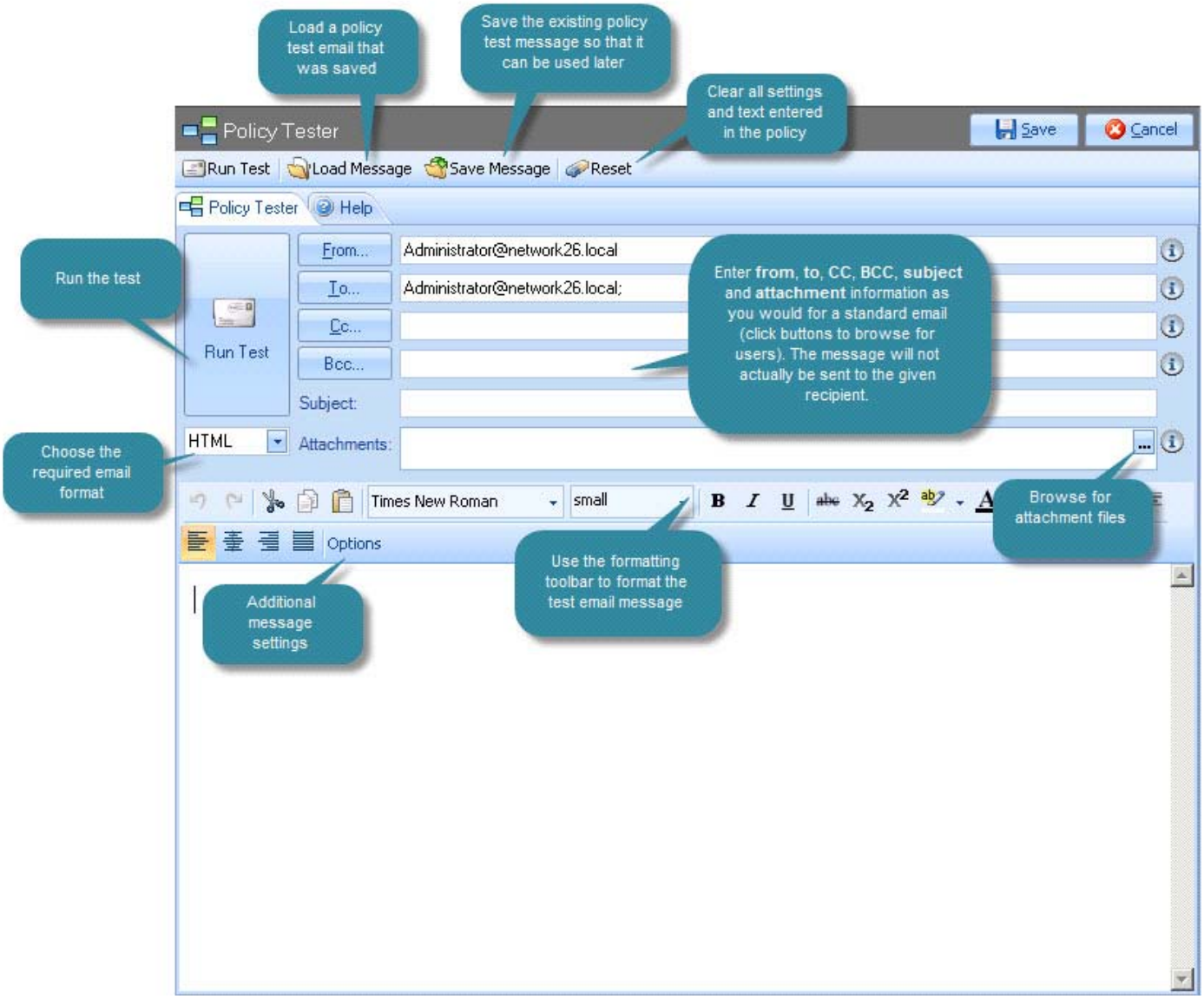
Then, having run a test, you access a process diagram [see page 158] and:

- View which policies have and have not been applied [see page 158]
- Check the reason why a policy is or is not applied [see page 160]
- Preview the message at any stage in the process [see page 161]

Finally, you can view original messages and their final output [see page 162].

Understanding the Policy Tester Window

The policy tester is designed to emulate Microsoft Outlook as closely as possible, so it will be familiar to most users:



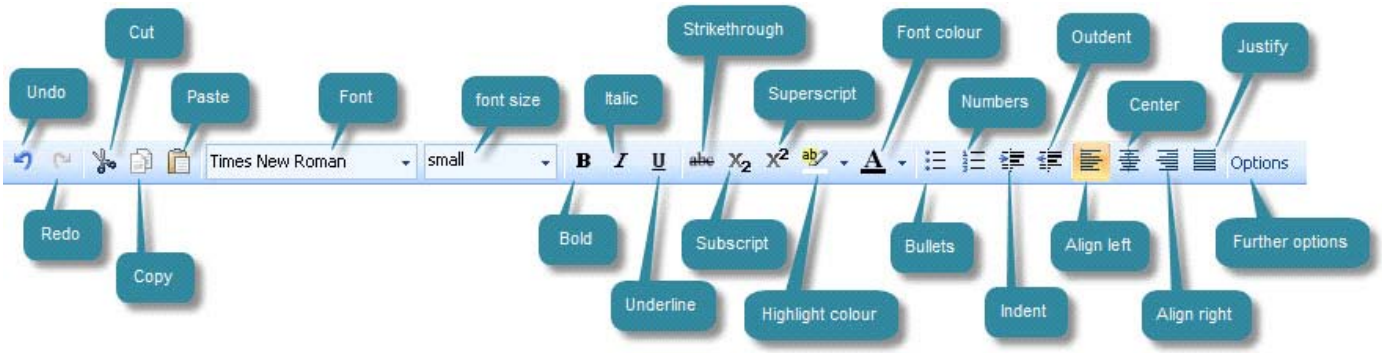
The upper section provides access to the policy tester toolbar [see page 154], and is used to define standard email details (such as sender and recipient) and the lower section contains an editor, so you can type the body of the test email. From here you can create a new message [see page 156] using the editor, save a message for re-use [see page 157], or load a previously saved message [see page 157] for testing.

The Policy Tester Toolbar

Toolbar option	Summary
Run Test	Having set required test criteria, use this option to run the current policy test (or use the large run test button in the main section of the policy tester)
Load Message	Rather than create a new policy test, choose this option to re-use a previously saved test [see page 157].
Save Message	Having set required criteria, use this option to save the existing test for re-use [see page 157].
Reset	Use this option to clear all settings in the policy tester and start from a 'clean' point.

The Email Editor Toolbar

The policy tester editor incorporates familiar word processing functionality, using a formatting toolbar:



Additional Options

The policy tester is designed to emulate Microsoft Outlook as closely as possible, therefore additional options are provided so that you can test the full range of Outlook options. When the options button is selected from the editor toolbar, additional message options are displayed, as summarized below:

Security Settings

- Choose to encrypt message content and attachments - the message is not actually encrypted but the Policy Tester emulates the process of doing so
- Choose to add digital signature to this message - a signature is not actually applied but the Policy Tester emulates the process of doing so

Message Settings

- Set the importance level to low, normal or high
- Set the sensitivity level to normal, confidential, personal or private

Delivery Options

- Specify an email address to have replies sent to
- Specify a send date (which will override the actual test date)

Headers

If you are testing a policy which is defined to apply an automated response based upon a specific email header, use these options to add that header to the test email.

Policy tester settings are retained (even if you exit Exclaimer Auto Responder) until you select the **reset** option from the policy tester toolbar [see page 154]. If you need to reset the policy tester, you can always save the current settings [see page 38]. for use at a later date, before doing so.

Creating a New Policy Test

To create a new policy test, follow the steps below:

1. Ensure that policies are in the correct sequence in the policy list [see page 67].
2. Select the policy tester.
3. Enter to and from information.
4. Enter CC and BCC information, if required.
5. Add attachments, if required.
6. Choose whether to test the email in HTML, RTF or plain text format.
7. Compose and format required email text in the policy tester editor [see page 153].
8. Set security, delivery and header options, if required (via the options button on the toolbar [see page 154])
9. Select the run test option.

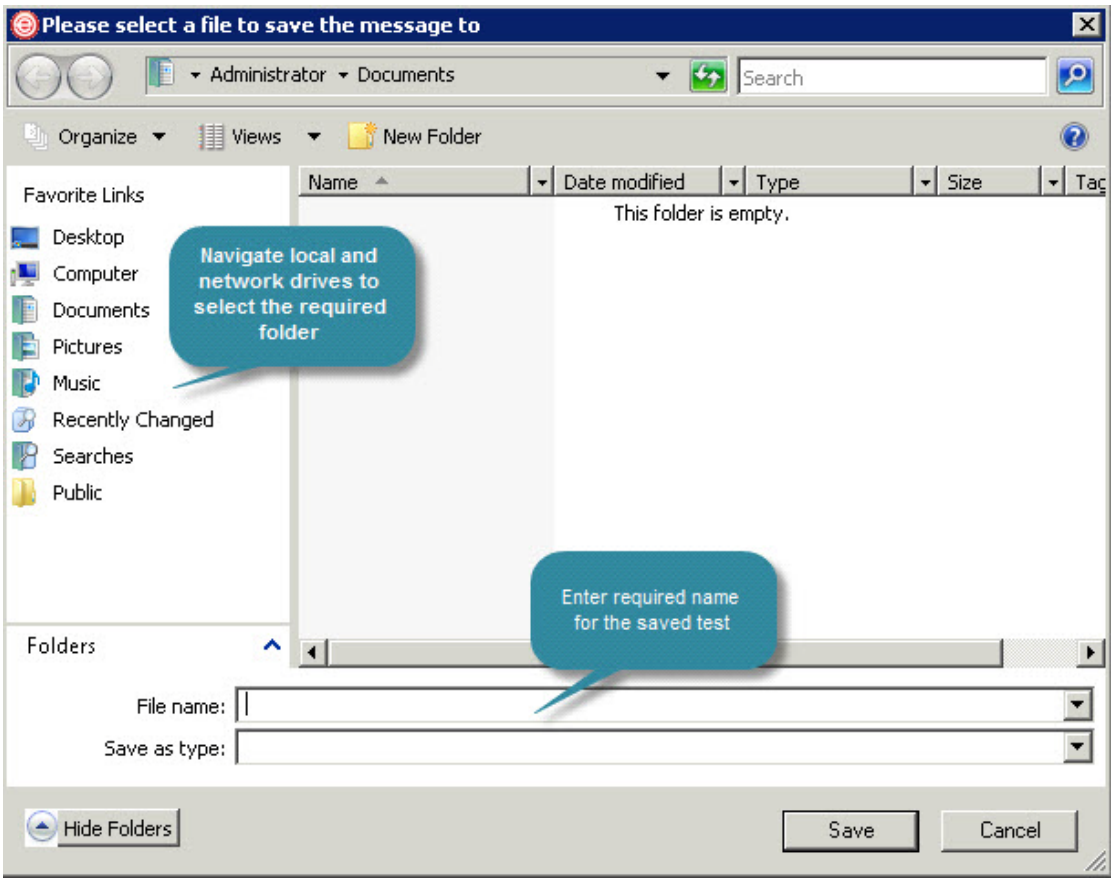
Policy tester settings are retained (even if you exit Exclaimer Auto Responder) until you select the **reset** option from the policy tester toolbar [see page 154]. If you need to reset the policy tester, you can always save the current settings [see page 38]. for use at a later date, before doing so.

Saving and Re-Using a Policy Test

Policy tester settings are retained until you select the reset option from the policy tester toolbar [see page 154], or until you close the Exclaimer console. However, if you need to reset the policy tester, you can choose to save the current settings first, for use at a later date [see page 157].

Saving a Policy Test

To save a policy test, ensure that options are set as required and click save message from the policy tester toolbar [see page 154]. Next, choose a location and filename for the saved policy test:



Re-using a Saved Policy Test

When a saved policy is loaded into the policy tester, fields within the policy are automatically populated with settings from the saved file.

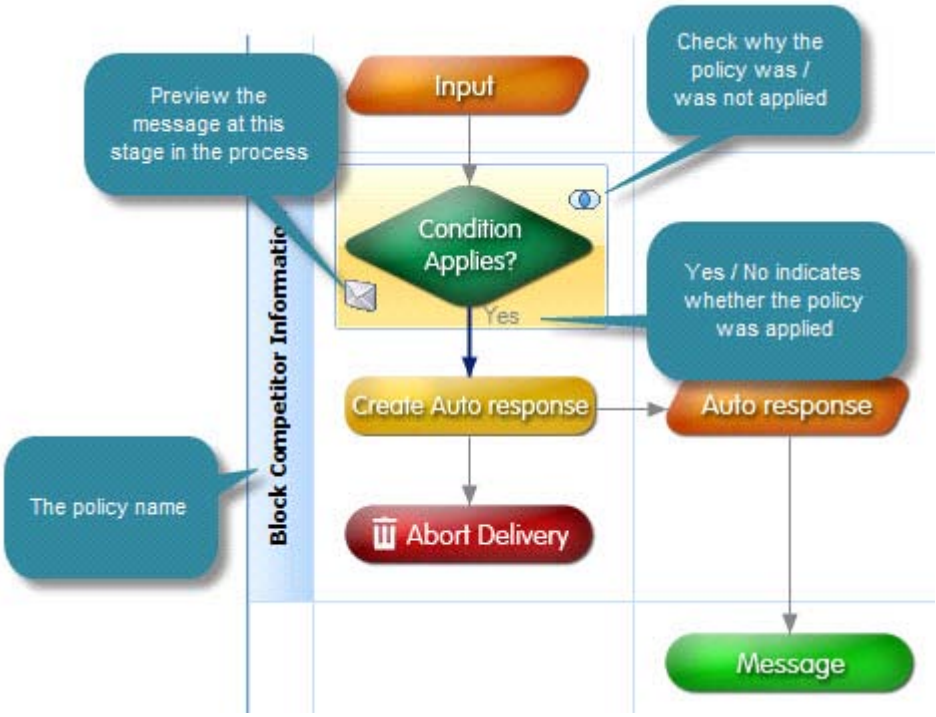
To load a saved policy into the policy tester, click the load message button from the policy tester toolbar [see page 154], and then navigate drives and folders to select the required policy test file.

Saved policy test files have an .MDM file extension.

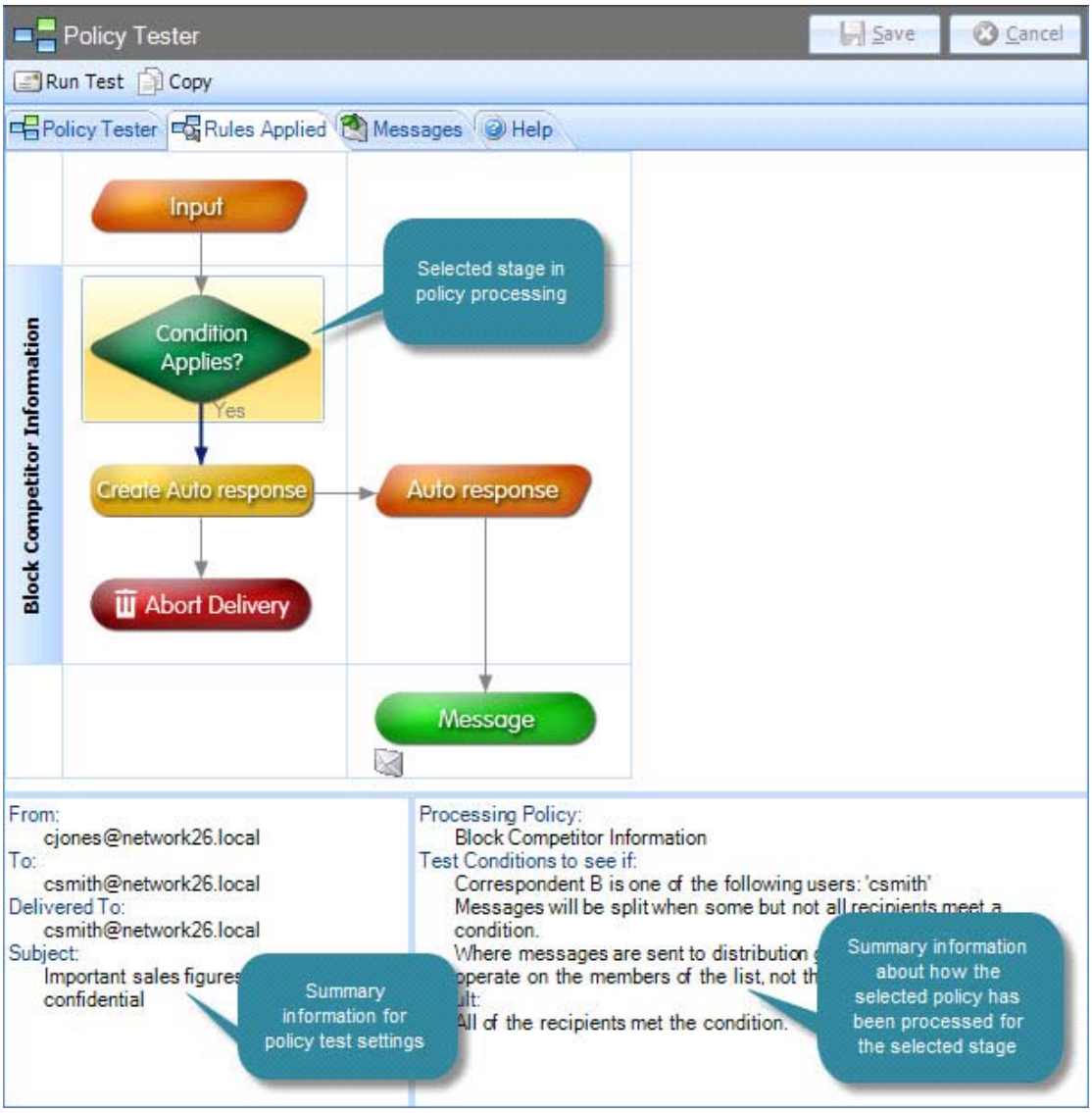
Working with Rules Applied Information

Having run a policy test, an additional tab named rules applied is displayed:

From here, you can view the outcome of the policy test as a process diagram. Here, each policy processed is displayed with a yes or no indicator, so you can see if the policy was applied. When you position the cursor over a segment of the diagram, additional options are displayed:



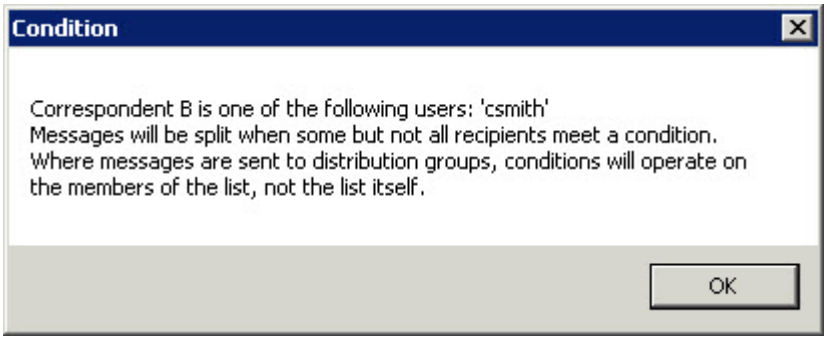
At the bottom of the rules applied window, summary information is available. From here, you can view basic settings for the policy test, and an explanation of how the selected policy has been processed (at the selected stage):



Checking the Reason Why A Policy Is or Is Not Applied

To view a brief summary of why a policy was or was not applied to the test message, hover the cursor over the relevant section of the process diagram until additional icons are displayed (as shown in the example above).

Click to view summary information - for example:

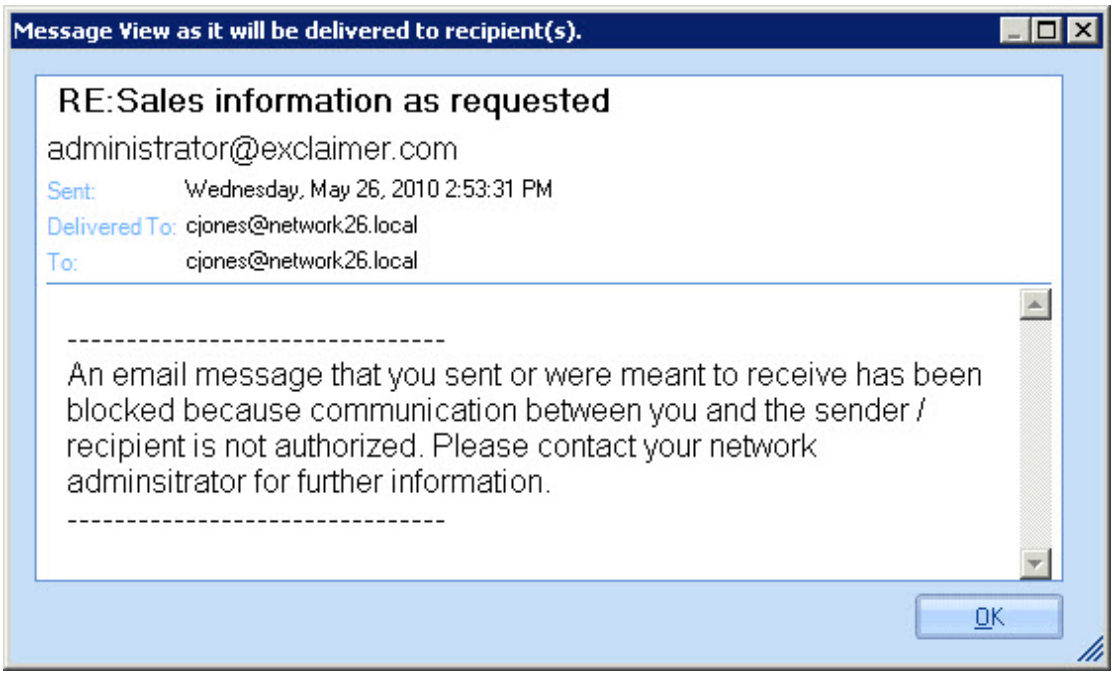


More detailed information is available at the bottom of the rules applied tab, as described in the previous section.

Previewing the Message at any Stage in the Process

To view a preview of the test email message at a particular stage of processing, hover the cursor over the relevant section of the process diagram until additional icons are displayed.

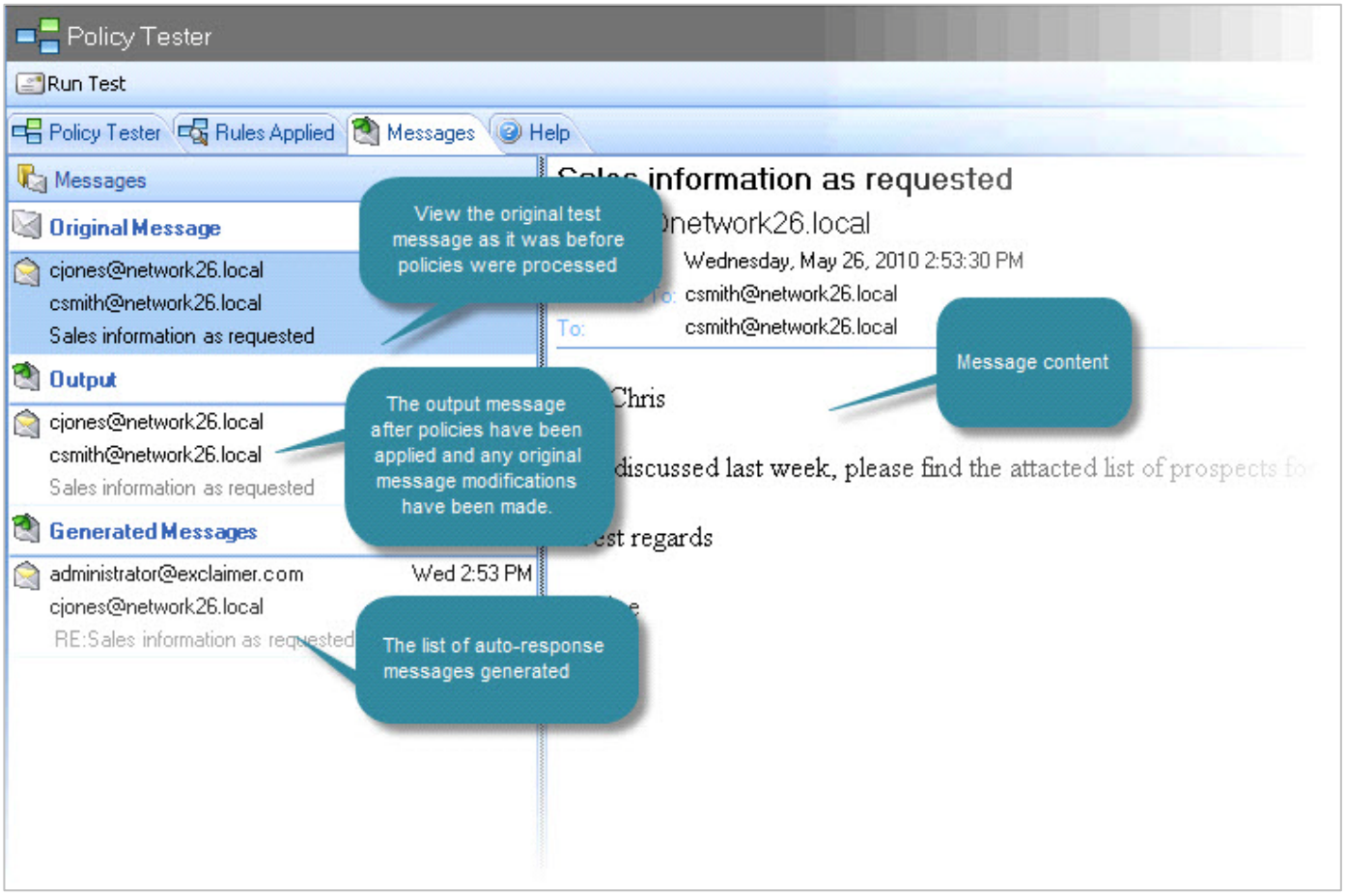
Click to view summary information - for example:



You can use the **copy** option on the toolbar to copy the data behind the process diagram to the Windows clipboard (for pasting into another application).

Working with Test Messages

Having run a policy test, an additional tab named messages is displayed. From here, you can view the original test message and also the final output:



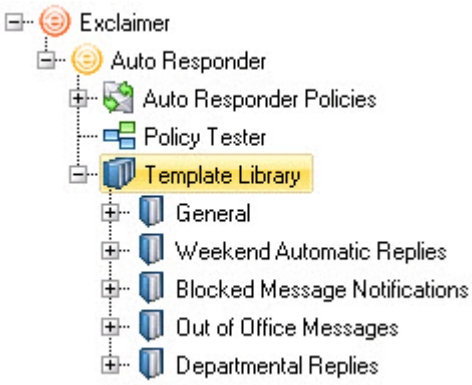
Chapter 6

The Template Library

Introduction

Templates are used to define the content of automated responses - for example, to compose automatic reply [see page 60] messages or to compose automatic notification messages to be used when a policy blocks transmission of a message [see page 62].

Within Exclaimer Auto Responder, all work with templates is completed using the template library (within the Exclaimer console [see page 16] tree):



A range of templates are included however, you can also create your own rich, sophisticated HTML layouts (including tables, images and dynamic Active Directory fields), together with simpler plain text versions.

Exclaimer Auto Responder sends automated replies in the same format as the original email (if an email is received in Rich Text Format, it is converted to HTML in order to keep as much of the formatting as possible). For this reason, you are advised to create each template in both HTML and plain text formats. If required, you can define templates to be applied before or after original email content [see page 191].

The template library is organized using categories, so that templates of the same type are grouped. When the topmost branch (template library) is selected, you can browse templates and work at category level. Below this, you can select specific categories to browse, edit and add templates.

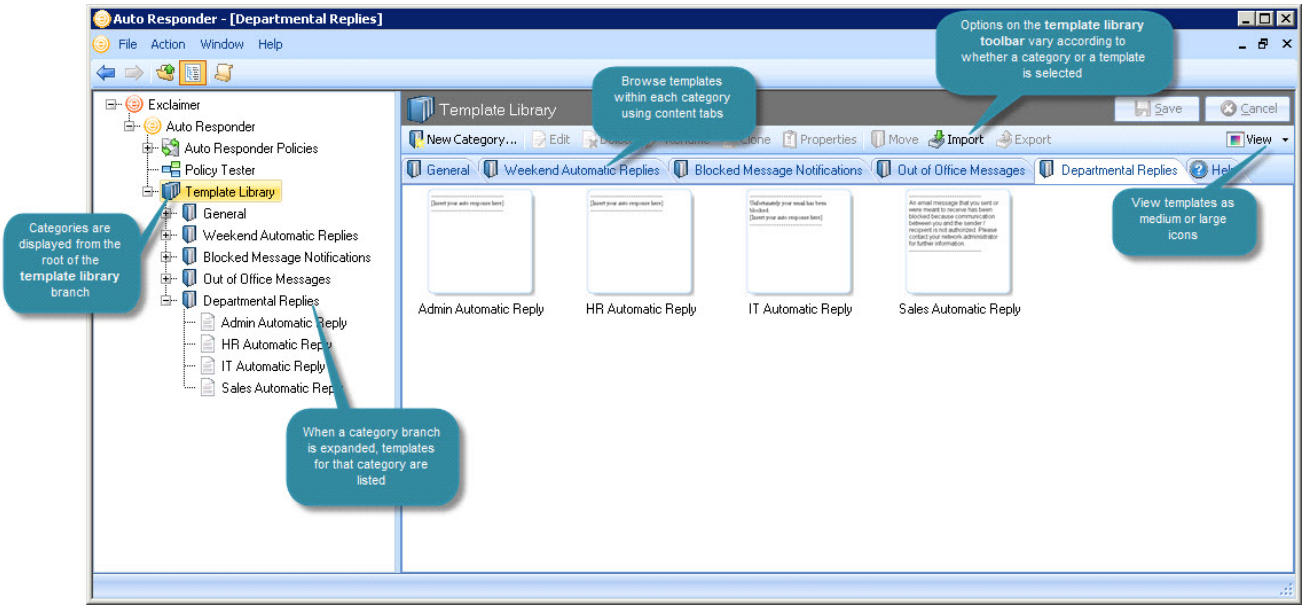
This section explains how the template library is used, including:

- Understanding the Template library window [see page 165]
- Working with categories [see page 169]
- The template editor [see page 184]
- Adding a new template [see page 175]
- Cloning a template [see page 177]
- Exporting a template [see page 178]
- Importing a template [see page 178]
- Editing a template [see page 179]
- Renaming a template [see page 180]
- Moving a template [see page 181]
- Viewing template properties [see page 182]
- Removing a template [see page 183]

You can also learn more about specific tasks, using the how to section for templates [see page 229].

Understanding the Template Library Window

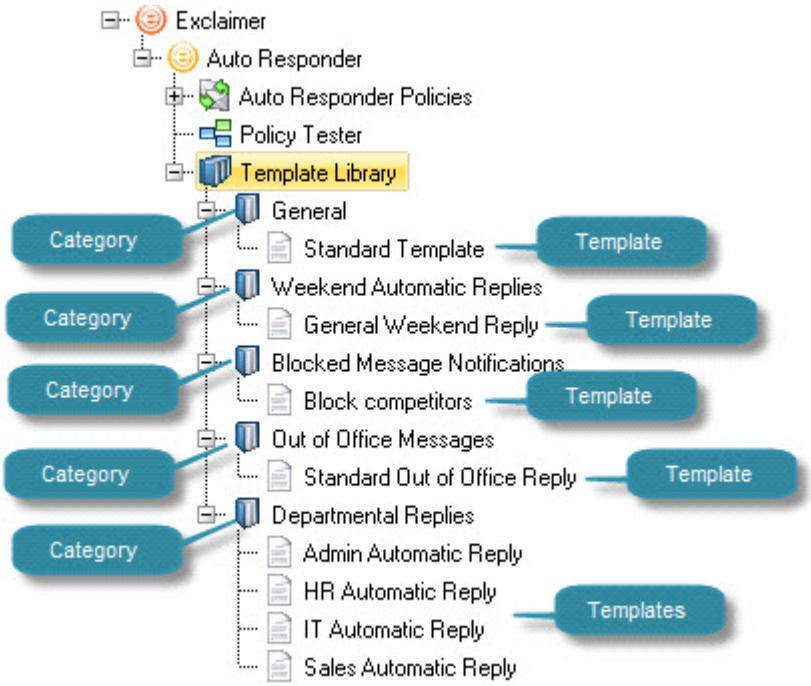
When the template library branch is selected in the console tree, you can browse templates and work at category level:



Options and actions [see page 167] are summarized in the following sections.

The Console Tree

When the top level (template library) branch is selected in the console tree, any template categories are shown as child branches, followed by templates within those categories:



The Template Library Toolbar

The template library toolbar provides quick access to key tasks. Options on this toolbar vary, depending on which branch of the library is currently selected.

Those listed below are available when the top level (template library) branch is selected:

Option	Function	Notes
New Category...	Create new category [see page 170]	Adds a new category to the bottom of the tree
Import	Import a template [see page 178]	Previously exported template files can be imported into the template library.

The Template Library Content Pane

When the top level (template library) branch is selected, the content pane displays available categories as a series of tabs.

If a category is selected, templates within that category are shown in the content pane, and if a template is selected the content pane shows a preview of that template.

View Options

When a category is selected, use view options to show templates as medium or large icons.

Actions

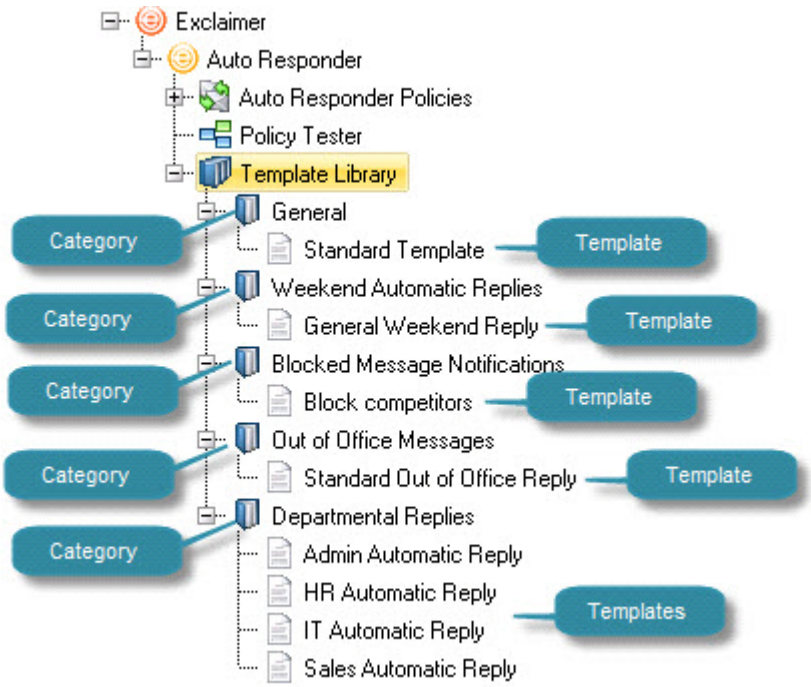
The following actions are available from the template library:

Action	Select this option to...
System	
Export configuration...	Export all settings and policies - see the export configuration... [see page 39] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [see page 39] page.
Licensing	Access the licensing tab to view licensing information [see page 27].
Auto Responder	
New policy	Launch the new auto responder wizard [see page 99] and choose from a number of scenarios to create a new policy (this option is particularly useful if you are not sure of the policy type [see page 60] required before starting).
Manage Auto Responder policies	Access the auto responder policies [see page 49] tab (and the same branch of the console tree) to work with policies [see page 57].
Status	View status information [see page 53] for Auto Responder.
New Policy Scenarios	
Automatic reply	Send an automatic response to emails. For example, if you are receiving a number of job applications and wish to send confirmation that emails have been received and are being processed.
Message redirection	Redirect messages to an alternative mailbox . For example, you may wish to redirect all messages sent to members of a team to the team manager, or if a staff member is on holiday you may wish to redirect their messages to someone who is covering them.

Action	Select this option to...
New Policy Scenarios (continued)	
Sender modification	Allow users to modify sender information. For example, members of a given department may need to choose whether to send an email from their own mailbox or from the general team mailbox.
Add recipients	Automatically add recipients to email messages. For example, you might require a copy of every message sent or received by a group of users to be discreetly sent to a monitoring mailbox for review by a manager. Alternatively, you might wish to automatically add a manager as a BCC recipient on all messages sent from a given employee.
Ethical walls	Prevent prohibited email communication. For example, your organization might include two departments where a conflict of interests could arise if communication between them occurs. In this situation, you can block email communication between these departments and (optionally) notify a compliance officer if a communication is attempted.
Advanced	Create a policy that is not based on a scenario - i.e. where no options are predefined.

Working with Categories

Within the template library, categories are used to organise templates into logical groups - for example, you might create a category for out of office replies, one for departmental replies, one for blocked email notifications and one for general templates:



At least one category must be defined to store templates. There is no right or wrong way to define categories - use whatever structure suits your organizational needs.

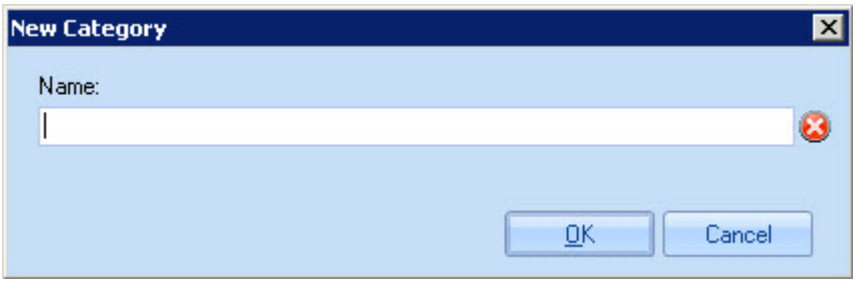
To view and browse existing categories, select the template library branch from the console tree. Existing categories can be viewed in the tree structure, or from the content pane [see page 167]. From here you can:

- Add a new category [see page 170]
- Rename a category [see page 171]
- Remove category [see page 172]

Adding a New Category

To add a new template category, follow the steps below:

1. Select the template library branch in the console tree.
2. Select the new category button from the toolbar, or right click and select new category from the context menu. You are prompted to enter a category name:



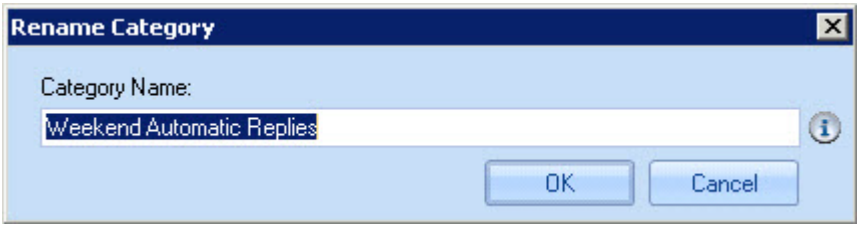
3. Enter the required name and click OK. The new category is added to the end of the categories list in the console tree.

When you are satisfied that all changes have been made correctly, click the main **save** button to save changes made in this session. Alternatively, use the **cancel** button to abandon all changes.

Renaming a Category

To rename a template category, follow the steps below:

1. Select the template library branch in the console tree.
2. Select the category to be updated.
3. Right click and select rename category from the context menu. The existing name is presented in editable form:



4. Update the category name and click OK.

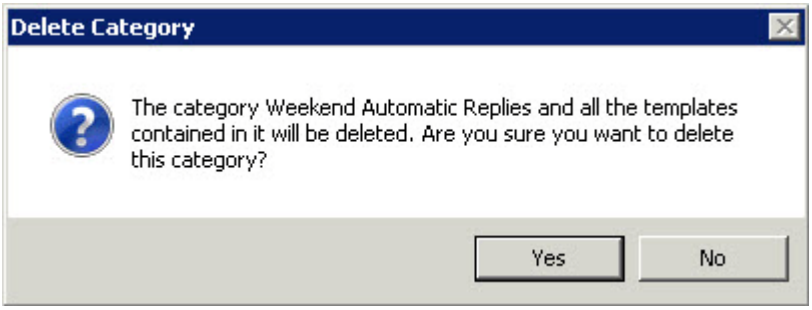
> When you are satisfied that all changes have been made correctly, click the main **save** button to save changes made in this session. Alternatively, use the **cancel** button to abandon all changes.

Removing a Category

It is important to note that removing a category will also remove any templates within that category. If required, you can move existing templates [see page 181] to alternative locations within the template library, or you may wish to rename [see page 171] the category rather than remove it.

To remove a template category, follow the steps below:

1. Select the template library branch in the console tree.
2. Select the category to be removed.
3. Right click and select delete category from the context menu. You are prompted to confirm that you wish to proceed:

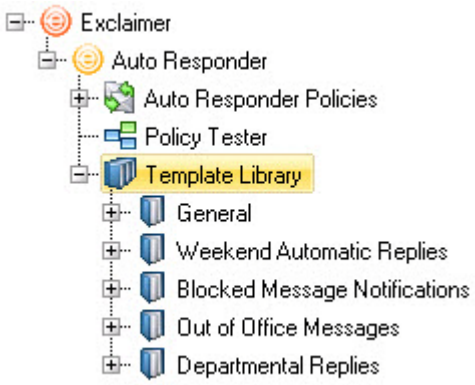


4. Click yes to remove the category.

> A category is not permanently deleted until settings have been saved. If you exit without saving (or **cancel** changes), the category will be reinstated in the console tree.

Working with Templates

All work with templates is completed within the template library [see page 165]. The appearance of the library will vary, depending on how you have chosen to organize templates into categories [see page 169]. For example:

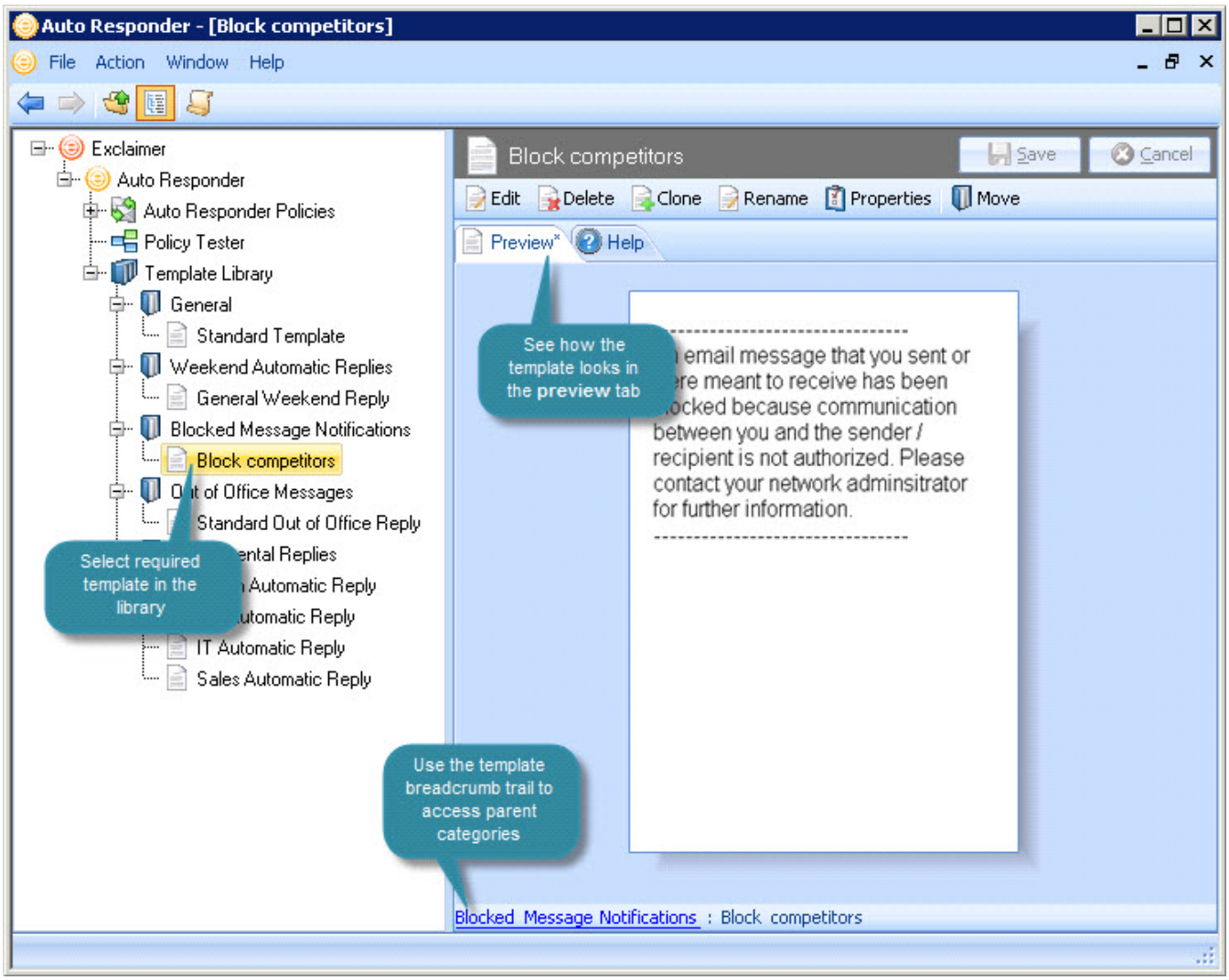


Having selected a template, you can preview and edit content in both HTML and plain text formats using an intuitive template editor, and of course you can add new templates to the library. This section explains how to work with templates, including:

- The template editor [see page 184]
- Adding a new template [see page 175]
- Cloning a template [see page 177]
- Exporting a template [see page 178]
- Importing a template [see page 178]
- Editing a template [see page 179]
- Renaming a template [see page 180]
- Moving a template [see page 181]
- Removing a template [see page 183]

Previewing a Template

To quickly see how a particular template will look when it is applied to email messages, simply select the required template from the console tree. The template is applied to a test message and displayed in the preview tab (within the content pane):



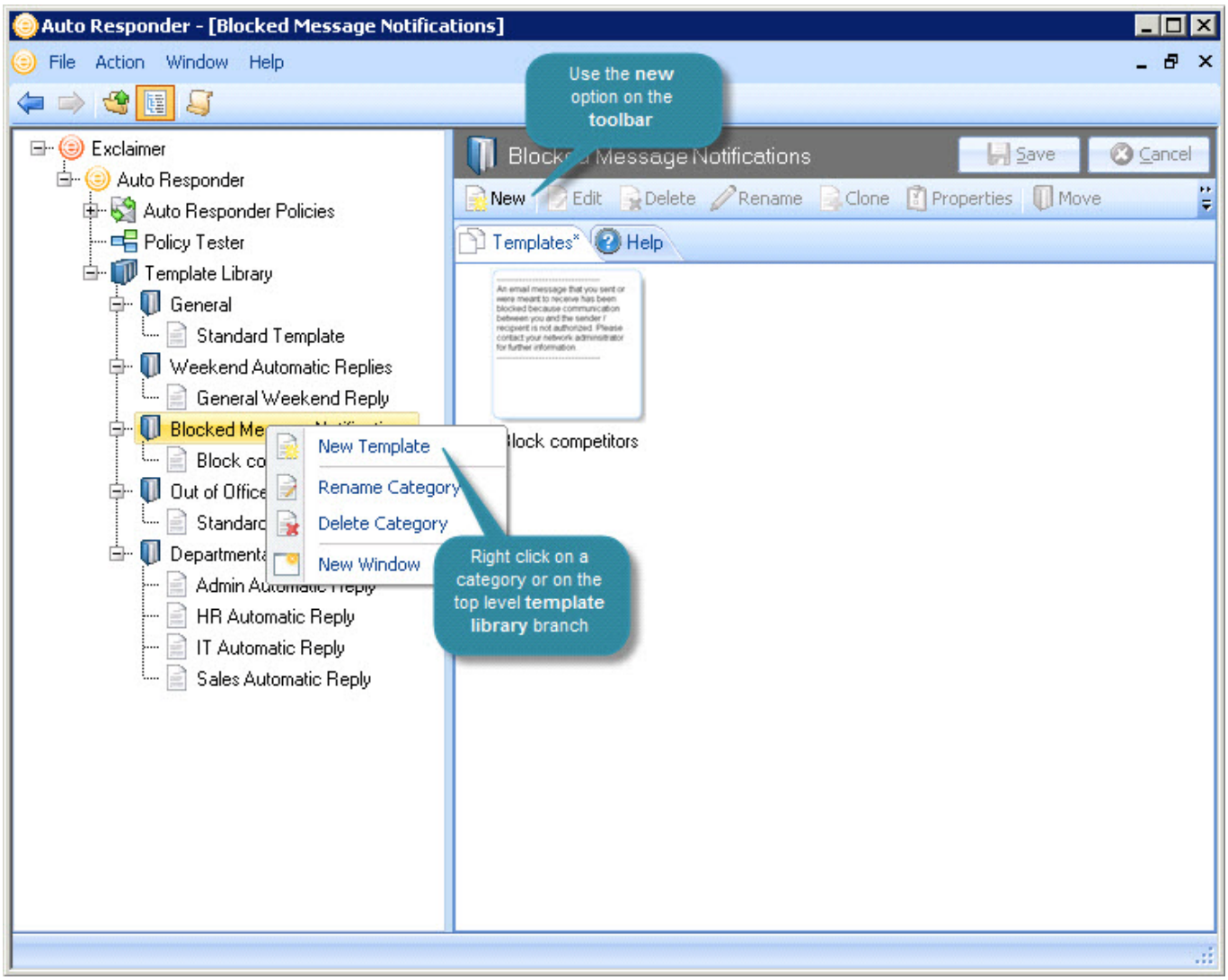
From here you can:

- Double click anywhere in the preview tab to edit the template [see page 179] in the template editor [see page 184].
- Select a template category [see page 169] from the template breadcrumb trail to view other templates in that category.
- Use toolbar options to edit [see page 179], delete [see page 183], clone [see page 177], rename [see page 180] or move [see page 181] the template.

> This **preview** option always shows the HTML version of the template. If you wish to preview the plain text version, you should choose to edit the template [see page 179] and select the **preview** mode for the required format.

Adding a New Template

The new template option is available from the console tree and from the toolbar:



To add a new template, follow the steps below:

1. Select the new template option to open a blank template in the template editor [see page 184]. At this stage, the new template is added to the template library with a temporary name. This name varies, depending on where the new template option was selected. If you added the template from a category, the temporary name will reflect the category name. If you started from the top level template library branch of the tree, the template is automatically assigned to the first category.

2. Create your template with required text and formatting. Remember that you can use tables, images, dynamic fields and properties when creating templates (see the template editor [see page 184] section of this guide for detailed information about editor options).

> If you wish to include the original message within automatic responses that uses this template, you will need to insert an original message field [see page 201].

3. Switch between HTML and plain text tabs to create the template in each format.

> Exclaimer Auto Responder sends automated replies in the same format as the original email (if an email is received in Rich Text Format, it is converted to HTML in order to keep as much of the formatting as possible). For this reason, you are advised to create each template in both HTML and plain text formats.
>
> If you attempt to save a template without creating a version in both HTML and plain text format, a warning is displayed. It is not mandatory to create both formats but creating two versions is recommended.

4. Click save and close (from the editor toolbar) to return to the template library.

5. If required, rename [see page 180] the new template.

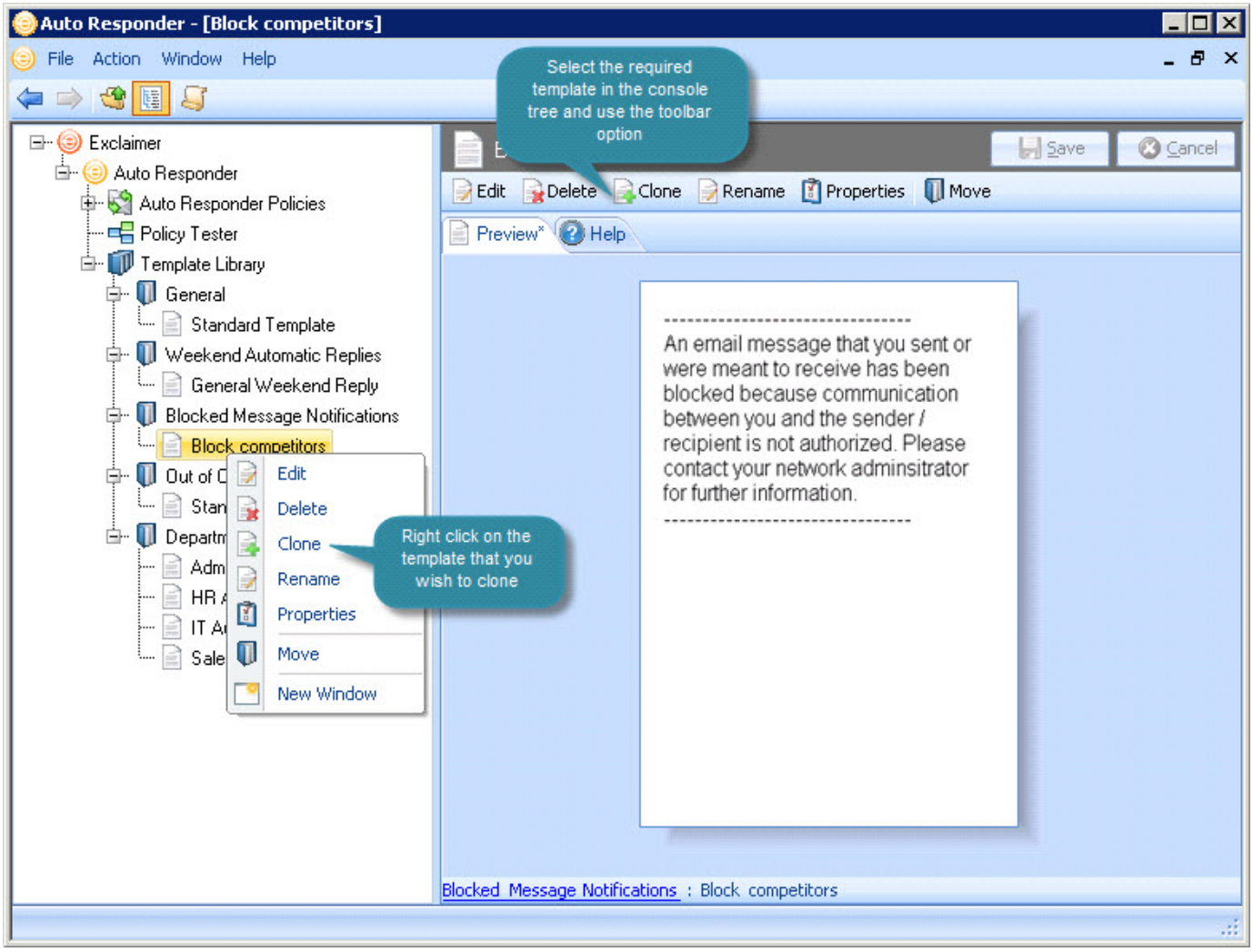
6. If required, move [see page 181] the template to a different category [see page 169].

7. Click the main save button to save changes [see page 38] made in this session. Alternatively, use the cancel button to abandon all changes.

Cloning a Template

If you need to create a new template which has similar settings to an existing template, it is quicker to take a copy of the existing template and then update that copy (as opposed to creating a new template from first principles [see page 175]).

The clone option is used to create a copy of an existing template for this purpose, and is available from the template library toolbar, the right-click menu and the actions pane:



To clone an existing template, select the template to be copied from the console tree, then either click clone from the toolbar or right click and select clone from the context menu. A copy of the selected template is added to the console tree, ready to be updated.

From here you can change the name [see page 180] and edit template content [see page 179] as required. Having updated the cloned template, click the main save button to save changes [see page 38] made in this session. Alternatively, use the cancel button to abandon all changes.

Exporting a Template

If required, you can export a template to a file. This is useful (for example) if you have chosen not to implement remote deployment [see page 34] and need to import a template [see page 178] on another server, or if you wish to delete a template but wish to take a copy first, just in case the template is needed in future.

To export a template, follow the steps below:

1. In the console tree, select the parent category for the template so that available templates for that category are displayed in the content pane.
2. In the content pane, select the template to be exported. Notice that import and export options are now activated on the toolbar.
3. Select export to open the save as window.

> The **file name** defaults to the name of the selected template and the **file type** is **.zip**. A **zip** file is used because there are multiple parts to a template file - it is not a single document.

4. Navigate drives and folders to select the required location for the template file.
5. Click save to complete the export.

Importing a Template

Previously exported [see page 178] template files can be imported into the template library. To do this, follow the steps below:

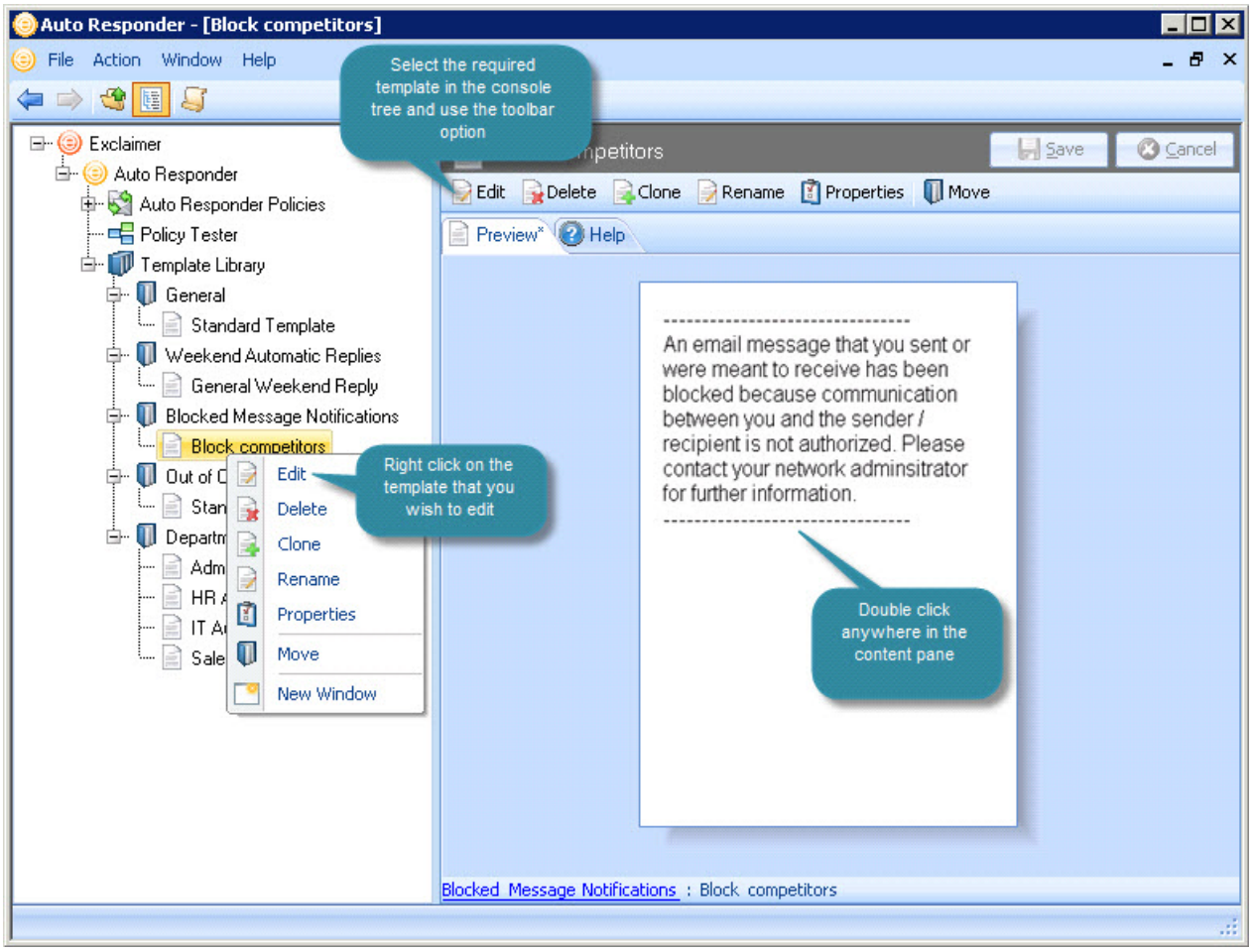
1. In the console tree, select a parent category for the template. Notice that import and export options are now activated on the toolbar.
2. Select import to display the open window.

> When a template is exported, the exported file format is **.zip**. Notice that the default file type here is set to **.zip**.

3. Navigate drives and folders to select the required import file.
4. Click open to complete the import and add the template to the template library.

Editing a Template

The edit option is available from the console tree, from the toolbar and by double clicking anywhere in the template preview pane:

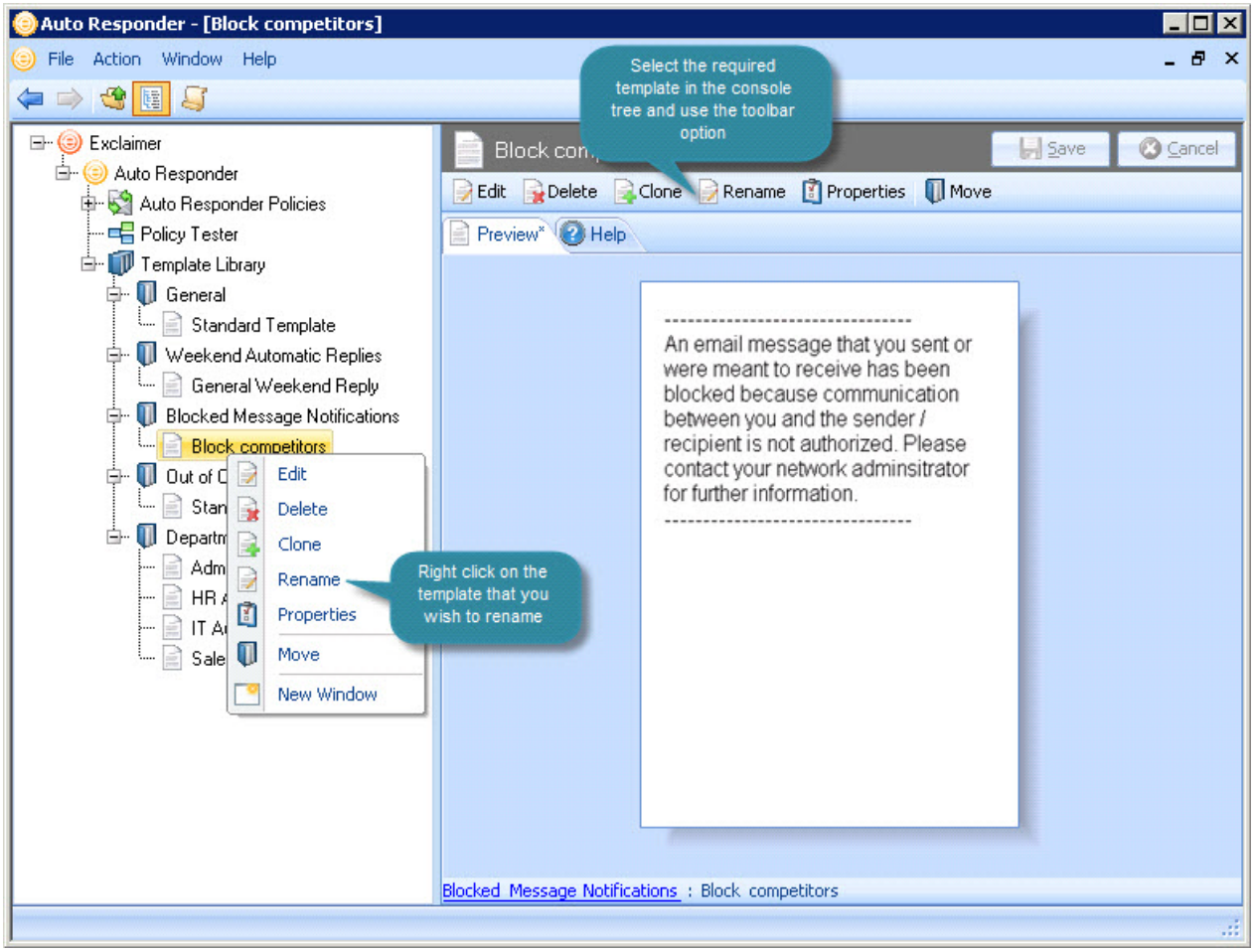


Having selected the edit option, the template is opened in the template editor [see page 184]. Simply make required changes, then click save and close (from the editor toolbar) to return to the template library.

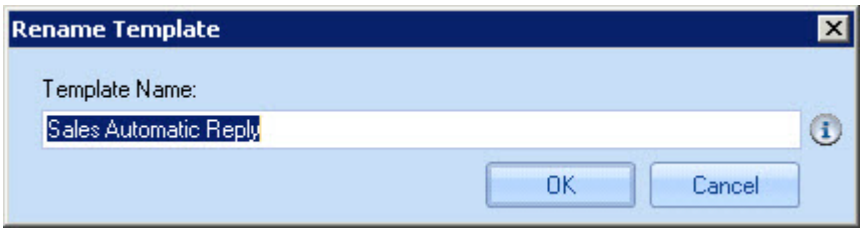
When you are satisfied with changes to the template, click the main save button to save changes [see page 38] made in this session. Alternatively, use the cancel button to abandon all changes.

Renaming a Template

The rename option is available from the console tree and from the toolbar:



Having selected the rename option, you are prompted to enter a template name:

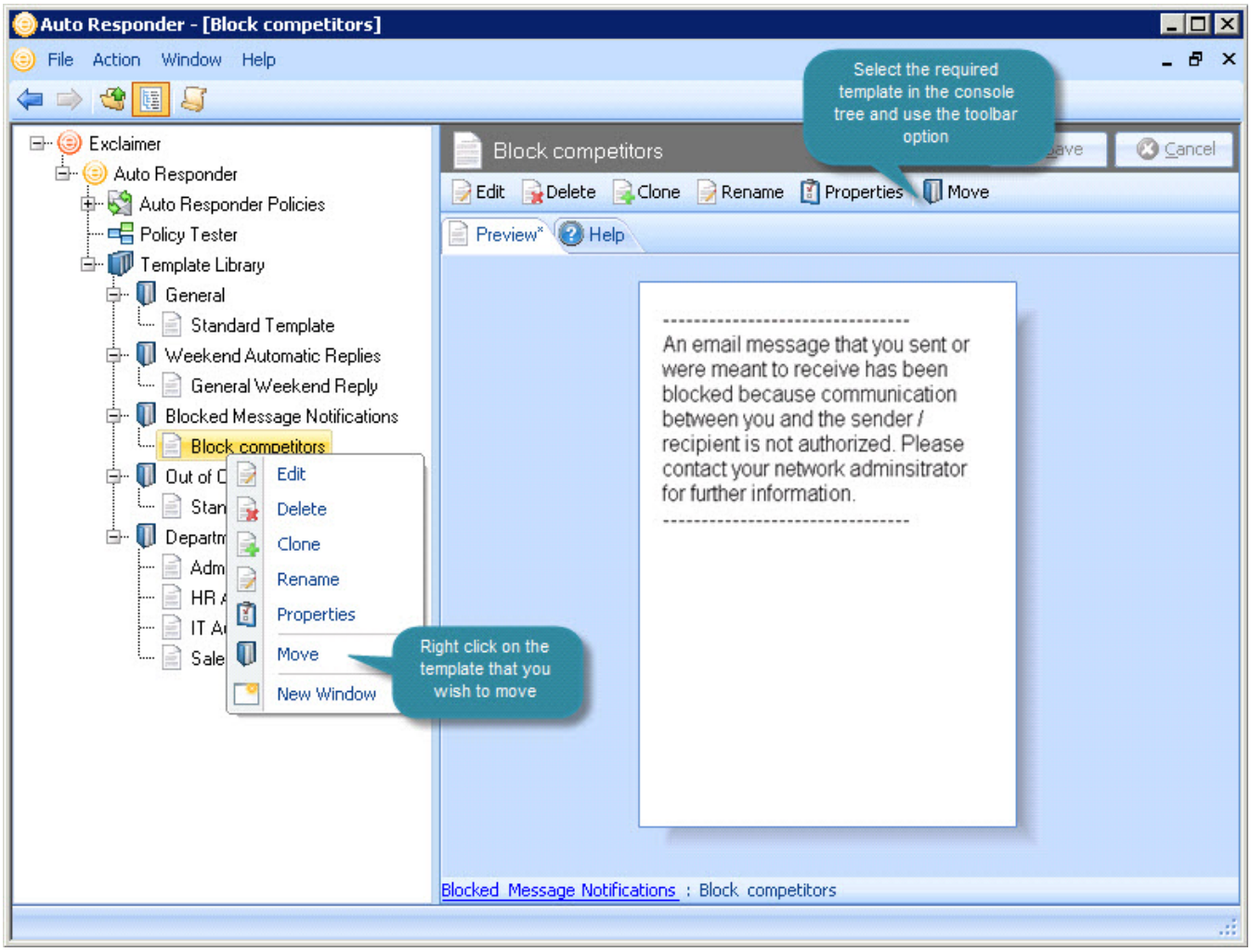


Simply enter the required name and click OK.

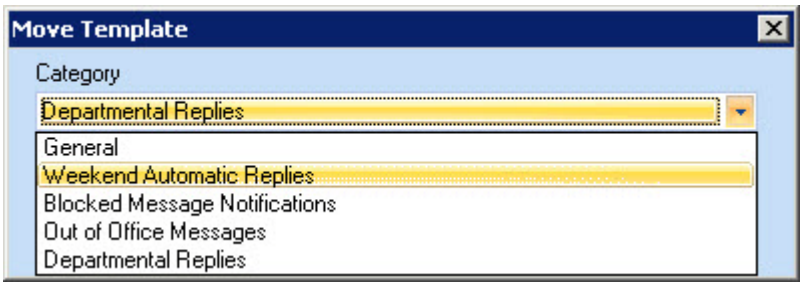
When you are satisfied that all tabs have been updated correctly, click the **save** button to save changes made in this session. Alternatively, use the **cancel** button to abandon all changes.

Moving a Template

Templates can be moved from one category to another using the move option, available from the template library toolbar and from the right-click menu:



Having selected the move option, a list of available categories is displayed:

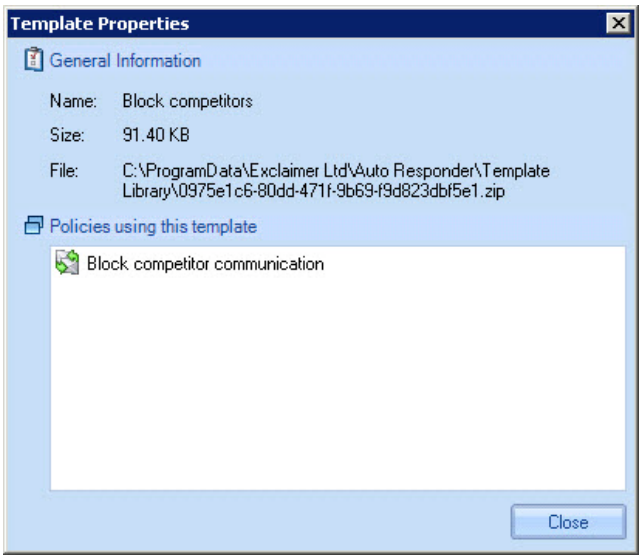


Select the required category and click OK to complete the operation.

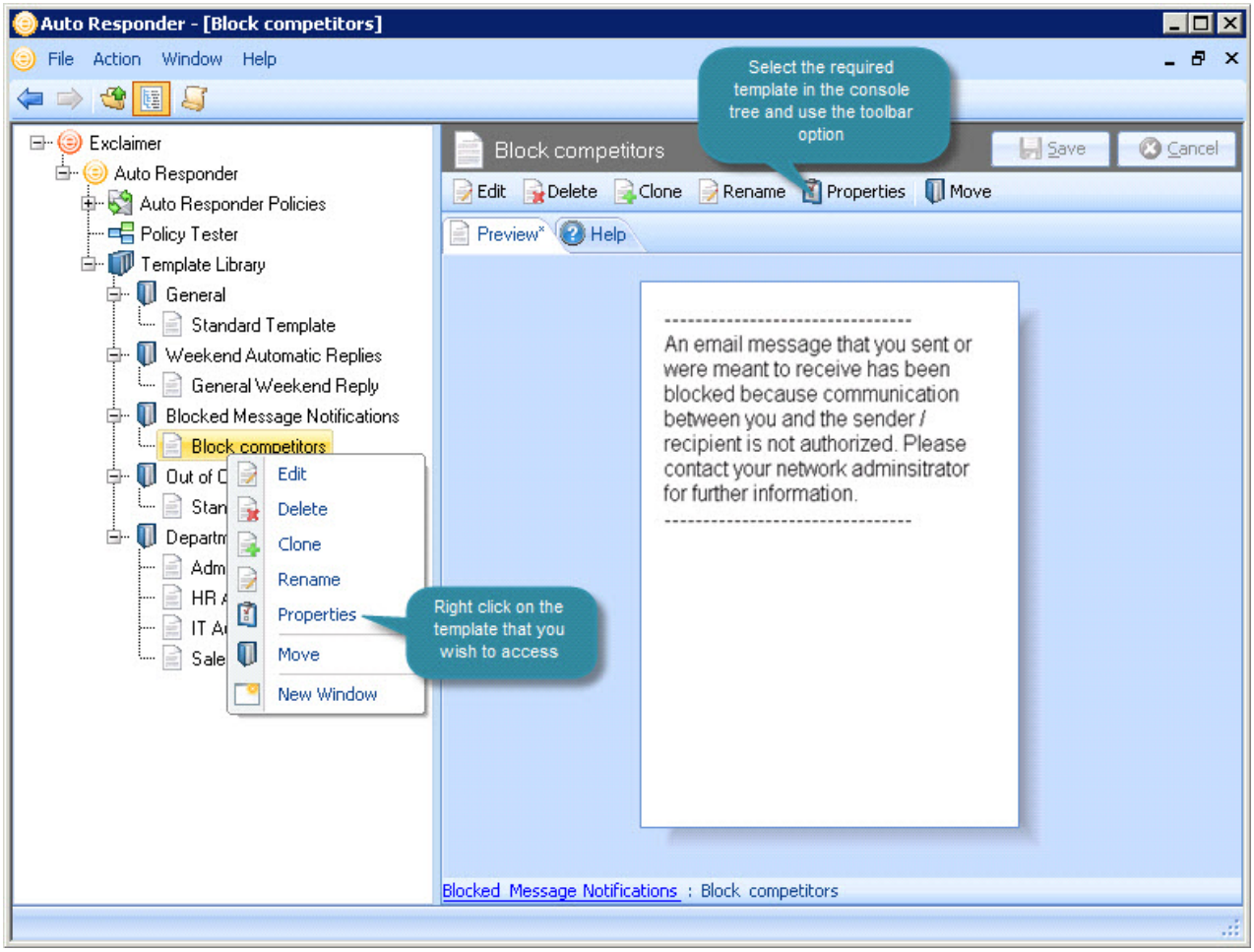
Click the main **save** button to save changes made in this session. Alternatively, use the **cancel** button to abandon all changes.

Viewing Template Properties

The template properties window shows general information about the template. From here you can see the template name, size and file location together with a list of policies that are using the template:

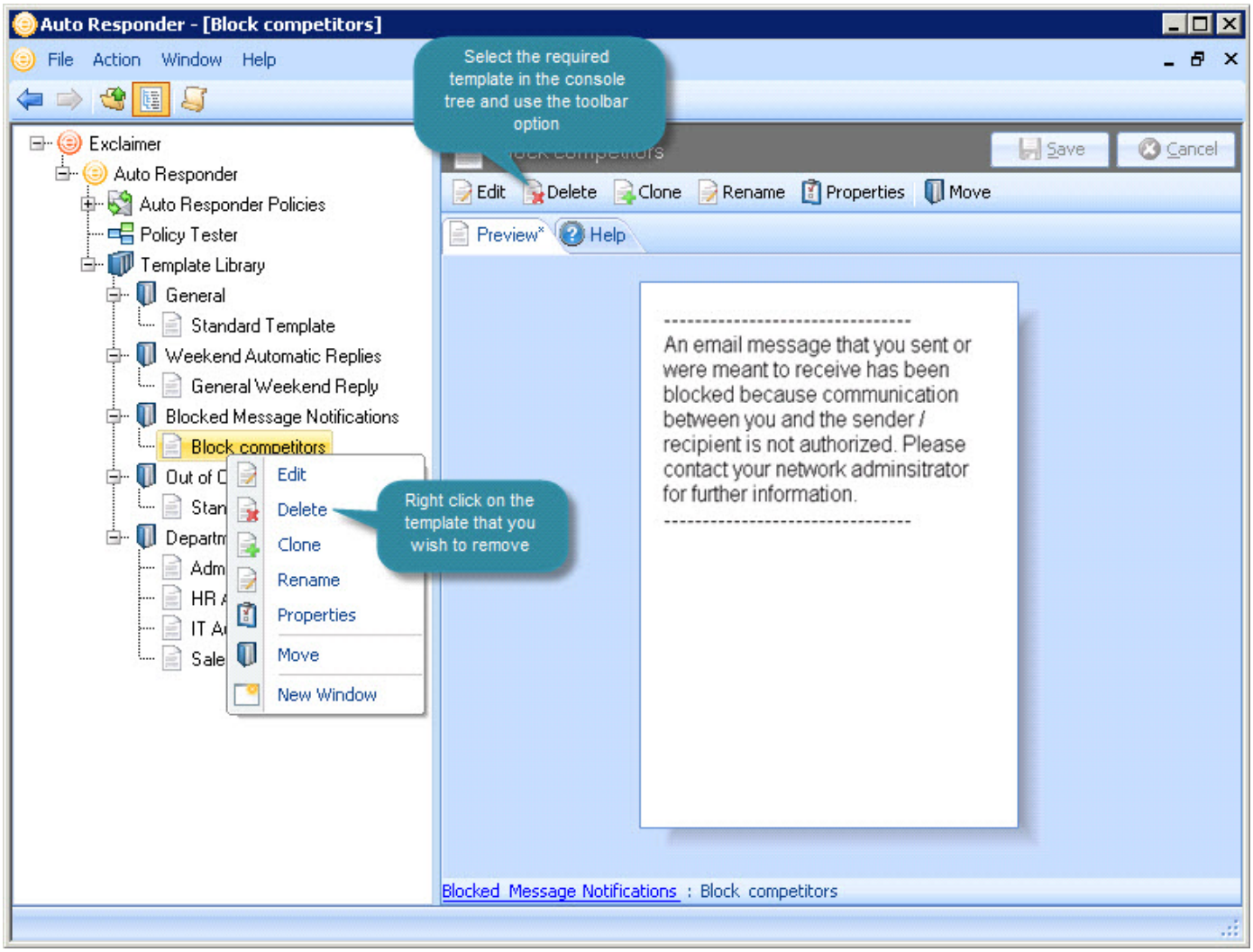


The properties option is available from the template library toolbar and from the right-click menu:

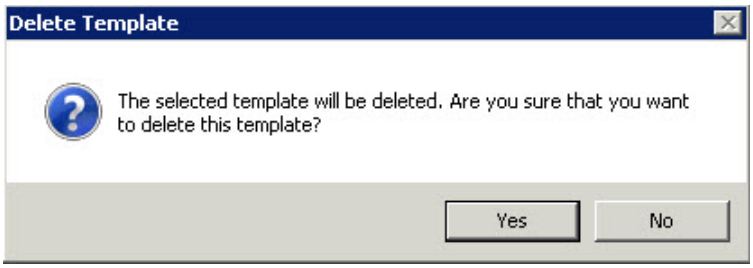


Removing a Template

Templates can be removed using the delete option, available from the template library toolbar and from the right-click menu:



Having selected the delete option, you are prompted to confirm that you wish to proceed:



Click yes to remove the selected template.

A template is not permanently deleted until settings have been saved. If you exit without saving (or **cancel** changes), the category will be reinstated in the console tree.

The Template Editor

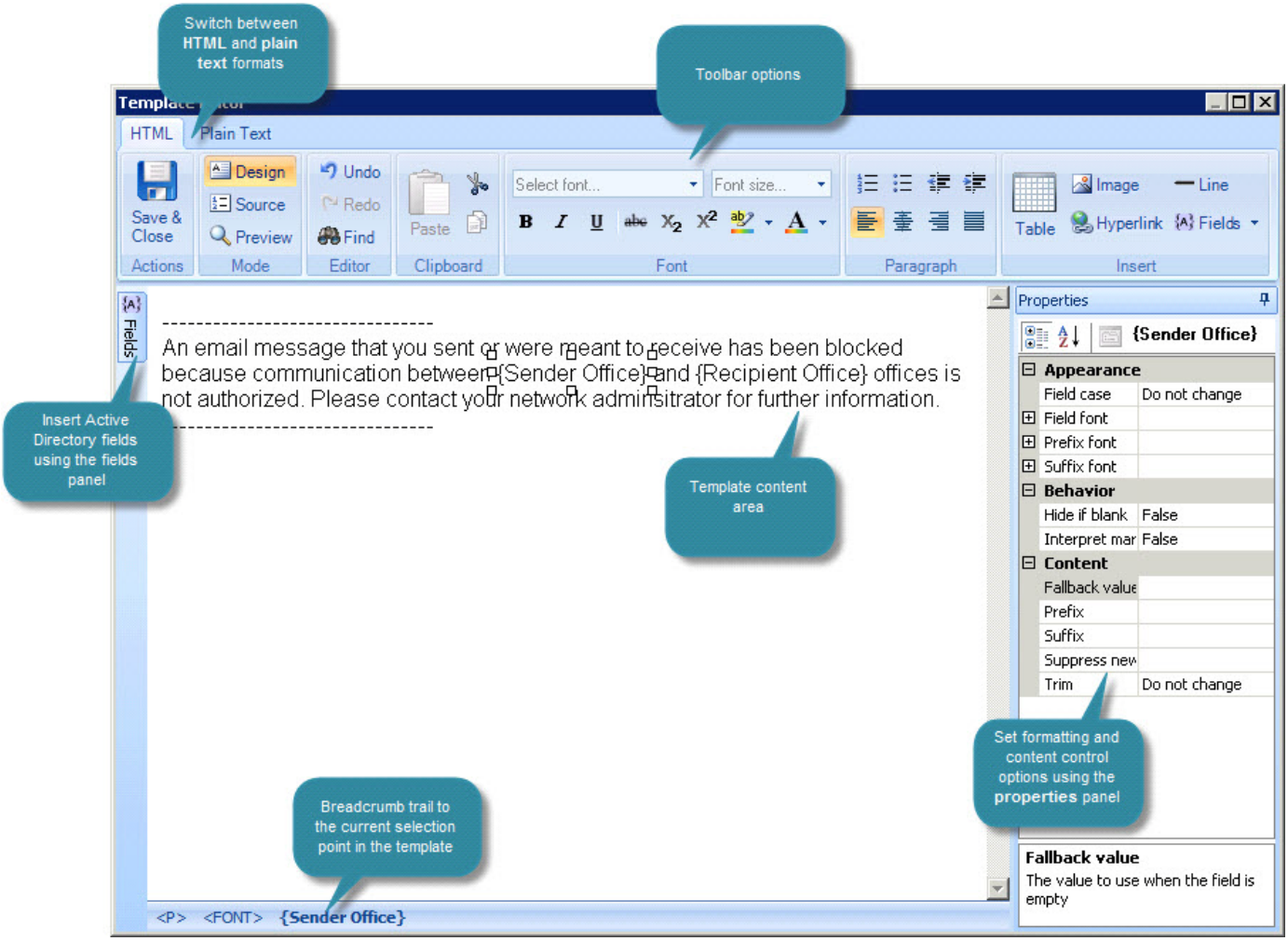
The template editor is used to add [see page 175], edit [see page 179] and preview [see page 174] templates in HTML and plain text formats. With a look and feel that will be familiar to Microsoft Outlook users, you can create templates which are as basic or as sophisticated as required.

This section provides an introduction to the template editor, including:

- Understanding the template editor window [see page 185]
- Template editor - toolbar variations [see page 188]
- Placement of content [see page 191]
- Fields [see page 198]
- Properties [see page 225]

Understanding the Template Editor Window

The template editor is used to add [see page 175], edit [see page 179] and preview [see page 174] templates in HTML and plain text formats:



The editor has a familiar, intuitive design, as summarized in the following sections.

The Content Area

All content is added to the main content area of the template editor. When you choose to add a new template [see page 175], the editor is opened with some placeholder text, which should be replaced with your required content. If you wish to include the original message within automatic responses that uses this template, you will need to insert an original message field [see page 201].

Switching Between Different Format Types

Tabs at the top of the editor are used to switch between different formats for a template (HTML and plain text). Exclaimer Auto Responder sends automated replies in the same format as the original email (if an email is received in Rich Text Format, it is converted to HTML in order to keep as much of the formatting as possible). For this reason, you are advised to create each template in both HTML and plain text formats.

The Template Editor Toolbar

If you are used to working with Microsoft Outlook, the template editor toolbar will be very familiar. When switching between format tabs, toolbar options will change, since some options are only applicable to a given format (for example, you can insert tables into HTML templates, but not in plain text versions). For a summary of the different toolbar options, see template editor - toolbar variations on page 188.

The Fields Panel

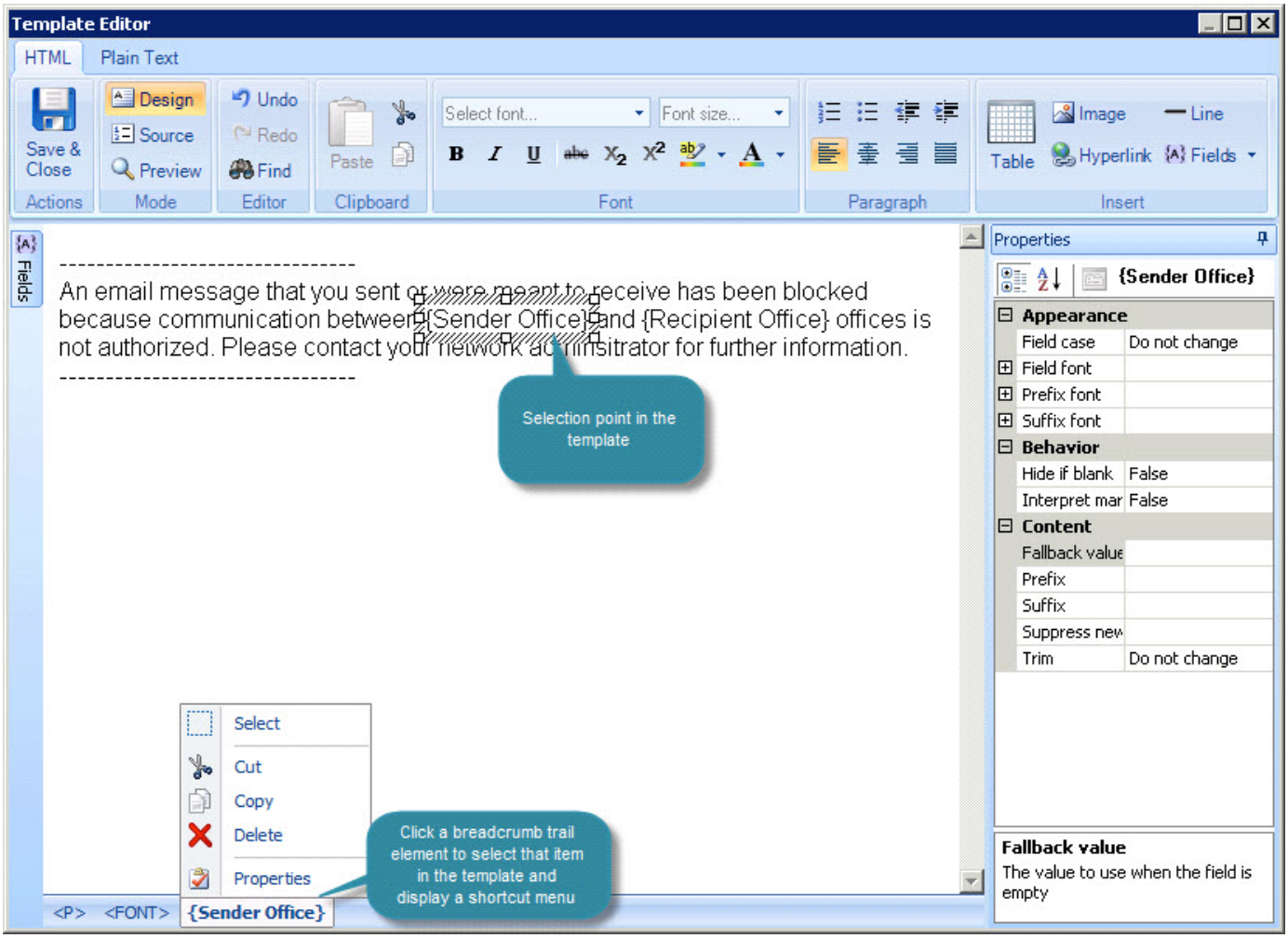
The fields option is used to insert dynamic content from the Active Directory. Click on the fields option to activate the fields panel - a list of available fields that can be inserted into the template. Once a field has been inserted this panel is automatically hidden so that the template editor is not cluttered. Fields can be used in both HTML and plain text formats. For further information, see the fields section of this guide on page 198.

The Properties Pane

Properties are used to format and control template content. Almost every piece of content added to a template will have properties associated with it - for example, text, tables, images, fields, hyperlinks, etc. The properties pane changes to reflect the current selection in the template editor - see the properties section of this guide on page 225 for further information.

Breadcrumb Trail

As you work with template content, the breadcrumb trail at the bottom of the editor window updates to show your current position. You can select any element in the trail to select that part of the template, and display a popup menu which contains shortcuts to key tasks - for example:



Toolbar Variations

When working with the template editor [see page 185], each template can be created in HTML and plain text formats. Exclaimer Auto Responder sends automated replies in the same format as the original email (if an email is received in Rich Text Format, it is converted to HTML in order to keep as much of the formatting as possible). For this reason, you are advised to create each template in both HTML and plain text formats.

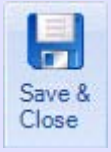
With Exclaimer Auto Responder, creating different versions of a template is made simple, using the HTML and plain text tabs at the top of the template editor. When a tab is selected, toolbar options are updated to show options that are relevant for that format.

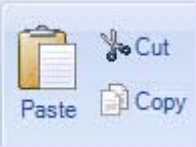
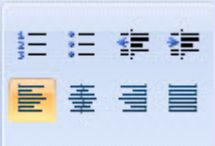
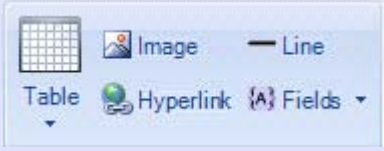
This section summarizes toolbar options for each format:

- The HTML editor toolbar [see page 188]
- The plain text editor toolbar [see page 190]

The HTML Editor Toolbar

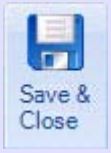
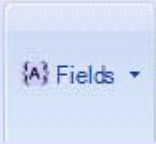
HTML templates can be sophisticated and feature-rich, utilising many of the options and techniques that you would expect from web pages (including tables, images, hyperlinks and dynamic content fields). When the template editor is set to HTML mode, the toolbar contains the following options:

Toolbar Option	Summary
	Save and close the current template and return to the template library.
	Mode options are used to switch between different view modes. Choose from: ▪ design - view and work with the WYSIWYG editor ▪ source - view and work with the HTML source ▪ preview - preview the template applied to a test message
	Editor options are used to perform key editorial tasks. Choose from: ▪ undo - undo the last action in the editor ▪ redo - redo the last action in the editor ▪ find - search for text in the editor

Toolbar Option	Summary
	Clipboard options are used to manipulate text. Choose from: ▪ paste - paste previously copied text at the current cursor position ▪ cut - remove currently selected text and copy it to the Windows clipboard ▪ copy - copy currently selected text to the Windows clipboard
	Font options are used to apply formatting to text. ▪ font name - select the required font from the drop-down list ▪ font size - select the required font size from the drop-down list Remaining options are summarized below, listed from left to right: bold, italic, underline, strike through, sub script, super script, highlight color, font color.
	Paragraph options are used to apply paragraph formatting. Options are summarized below, listed from left to right: numbered list, bulleted list, outdent, indent, align left, center, align right, justify.
	Insert options are used to apply more detailed formatting and interactive content. Options are (from left to right) insert table, insert image, insert horizontal line, insert hyperlink, insert fields.

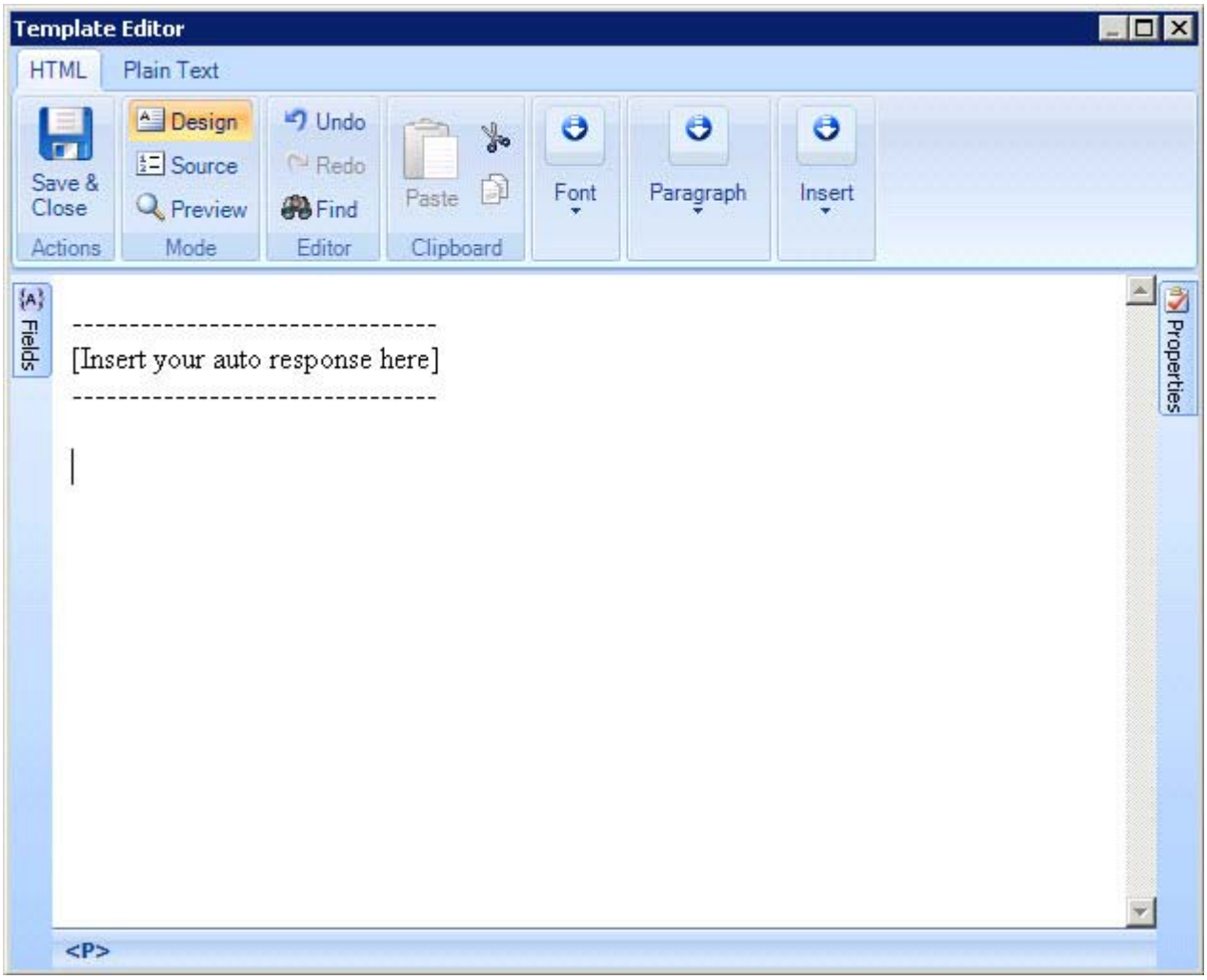
The Plain Text Editor Toolbar

Plain text templates are composed without any formatting information, however you can still include Active Directory fields [see page 198]. When the template editor is set to plain text mode, the toolbar contains the following options:

Toolbar Option	Summary
	Save and close the current template and return to the template library.
	Mode options are used to switch between different view modes. Choose from: ▪ design - view and work with the WYSIWYG editor ▪ preview - preview the template applied to a test message
	Editor options are used to perform key editorial tasks. Choose from: ▪ undo - undo the last action in the editor ▪ redo - redo the last action in the editor ▪ find - search for text in the editor
	Clipboard options are used to manipulate text. Choose from: ▪ paste - paste previously copied text at the current cursor position ▪ cut - remove currently selected text and copy it to the Windows clipboard ▪ copy - copy currently selected text to the Windows clipboard
	View options are used to help when working with plain text. Select the whitespace option to view paragraph markers within the editor and click word wrap to wrap text to accommodate the window size. These options do not change the way in which the template will be viewed by recipients.
	Insert options are used to insert dynamic content fields [see page 198].

Placement of Content

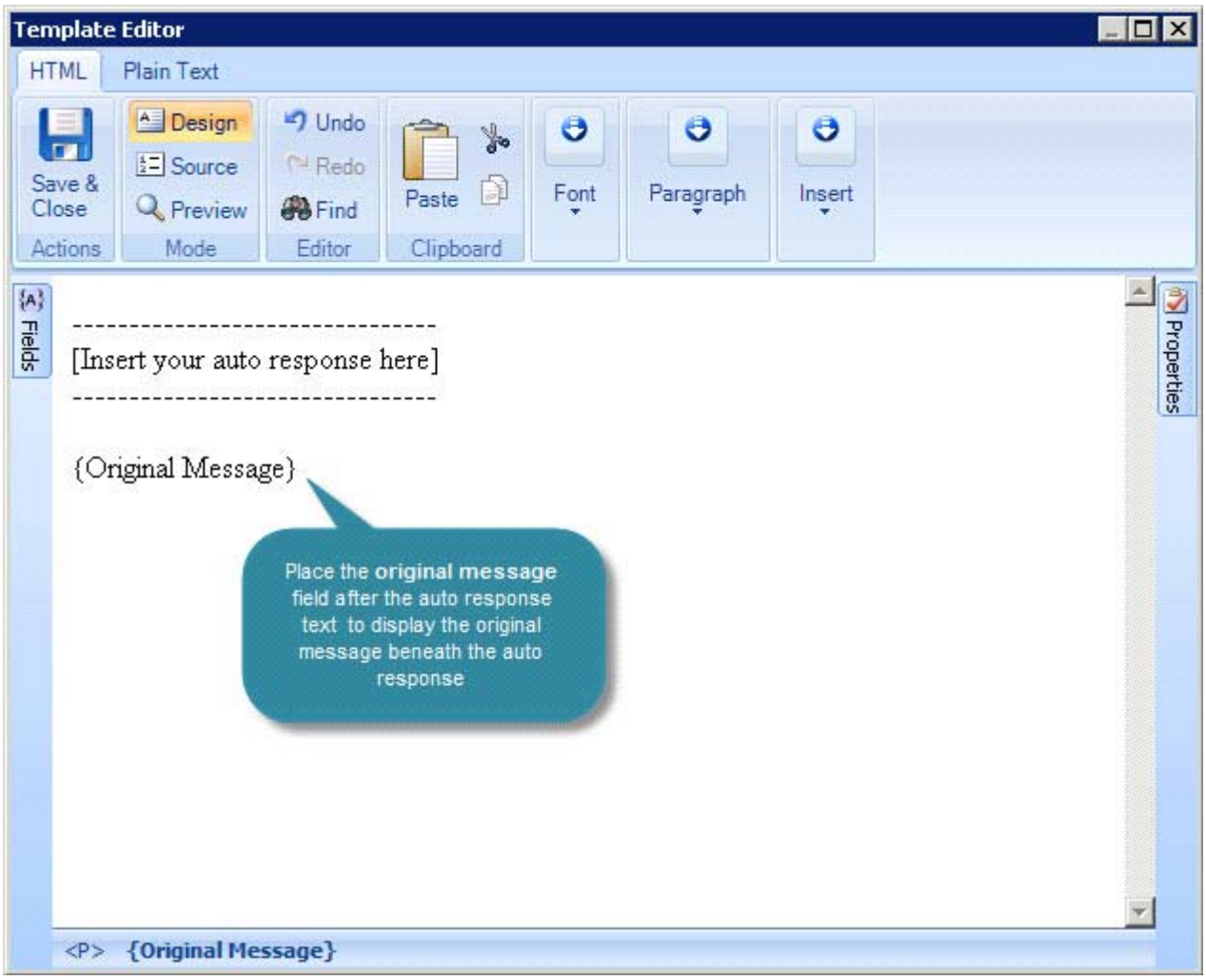
When creating a new template, an initial placeholder is displayed:



This placeholder should be replaced with the required content for the automatic reply.

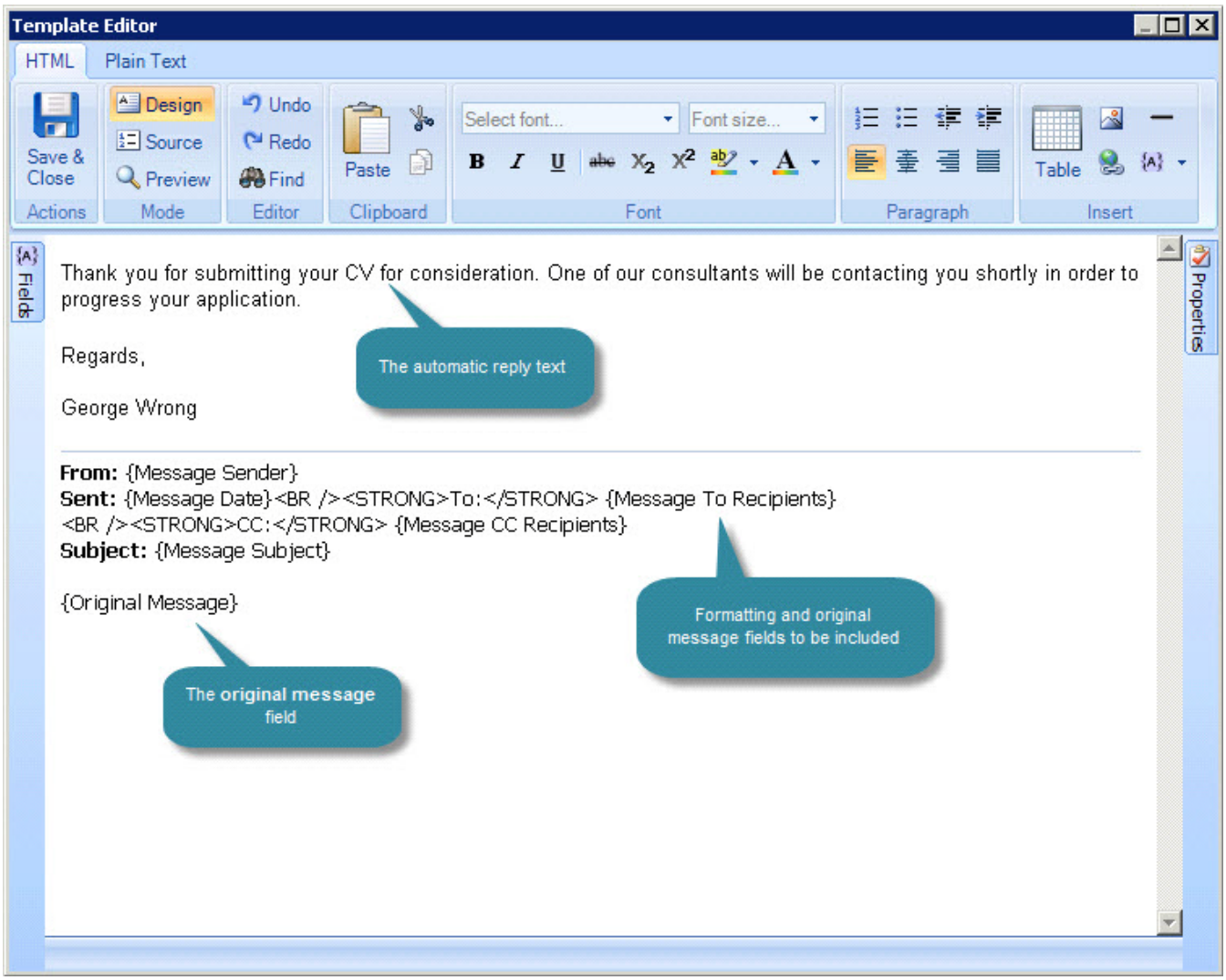
Including the Original Email in an Automatic Reply Message

If you wish to include the original email message in an automatic reply, you can add an original message field from the fields panel [see page 199]:



The original message field should be placed according to where you want the original message to be displayed, relative to the automatic reply.

For example:



If required, you can choose to attach a copy of the original message to an automatic reply. To do this, select the **attach original message** option on the auto response tab [see page 78] for the required policy.

Tips for Working with Original Message Fields

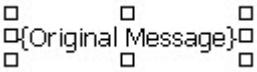
Using Spaces

The placement of content will be made exactly as displayed in the editor. For example, if you enter three blank lines between your automatic reply content and an original message field , there will be three blank links at the end of your automatic reply, followed by the original message.

Copying and pasting original message fields

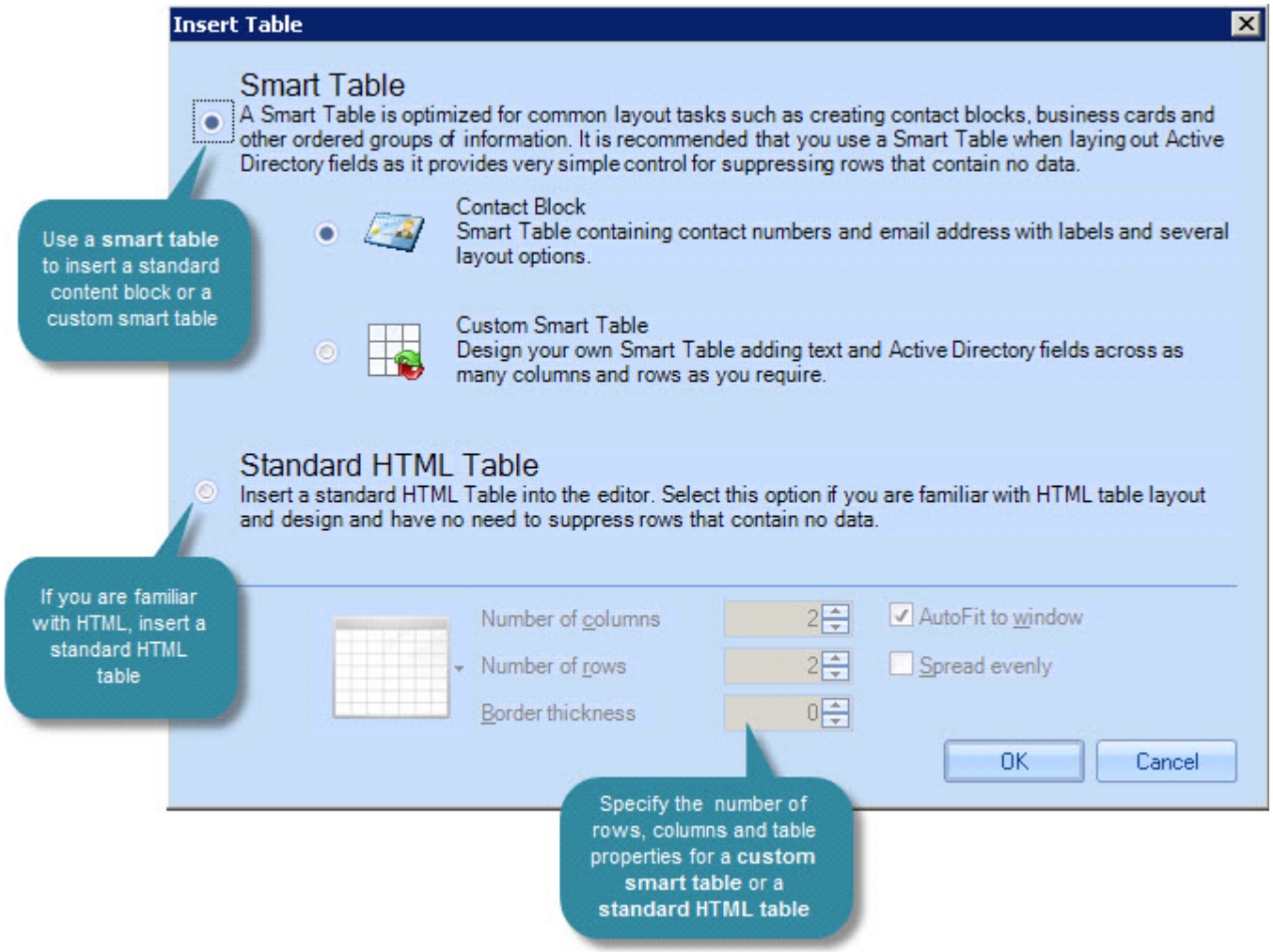
You can copy and paste original message fields to new positions within the template - care should be taken to ensure you copy/paste the entire field rather than just the text element. When you click on a field, it behaves like a table cell. For a correct selection, you should see the borders of the cell clearly marked:

...or



Tables

When working with HTML templates, selecting the table option from the editor toolbar displays an insert table options window:



From here, you can choose the type of table to be inserted - choose from:

- A smart table - contact block [see page 196]
- A smart table - custom [see page 196]
- A standard HTML table [see page 196]

These options are summarized in the following sections.

Smart Table - Contact Block

When working with templates, a common requirement is to insert standard contact information for the message sender. You can do this by adding individual fields [see page 198] to the template, but it can be neater and quicker to use a predefined contact block. A contact block is essentially a table of commonly used message sender [see page 202] fields - for example:

Tel:	{Sender Telephone number}
Fax:	{Sender Fax}
Mobile:	{Sender Mobile}
Email:	{E-mail (as hyperlink)}

A key benefit of using a contact block rather than individual fields is that you can choose to suppress a row if there is no information in the message sender's Active Directory information to include. For example, if a contact block includes a {fax} field but there are no fax details for a message sender, the 'fax' row of the block is not displayed when the message is sent,

Once inserted, a contact block can be edited - for example, you might wish to swap one field for another, or adjust the formatting (using properties [see page 225]). For further information, please see how do I create a contact block? on page 235.

> When the contact block is selected from the insert table options window, table rows and attributes are not available. This is because the contact block is a predefined table; however you can adjust the table once it has been inserted into the template.

Smart Table - Custom

The custom smart table option can be used to insert a table and specify content / attributes using straightforward data entry fields. This is a quick and easy way to insert a table and include Active Directory fields (or other content) at the same time; the alternative would be to insert a standard HTML table and add fields or other content manually.

For further information, please see the smart tables on page 221.

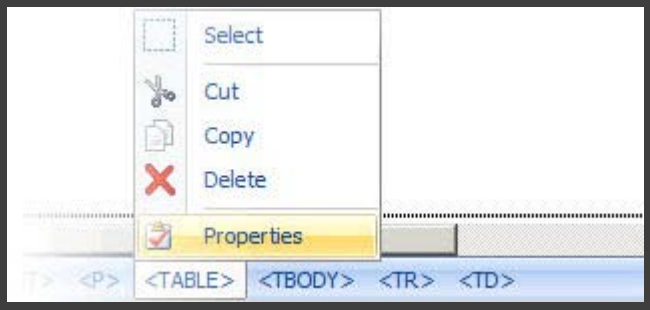
Standard HTML Table

If you wish to insert a standard HTML table and do not wish specify any content until after it has been added to the template, use the standard HTML table option. This is useful (for example) if you wish to insert a basic table to form the layout of a template, or if you wish to include tabular data which does not include fields.

Having selected the standard HTML table option from the insert table window, you can set the number of columns and rows, together with border, autofit and spread attributes. Then, click OK to insert the table and start to add content.

When working with any kind of table in the HTML template editor, it may be useful to note the 'HTML element trail' at the bottom of the editor window.:

Depending on the size of your table, it can sometimes be tricky to select a particular row, column or cell, but you can do this very easily from the element trail - just click the required element. When you click on an element, further options are displayed:



Selecting properties will show properties for this table element in the properties pane [see page 225].

Using Fields in Templates

Automatic reply content can include a wide range of dynamic information using Active Directory fields. These fields are inserted into templates (via the template editor) and then dynamically updated when messages are sent or received.

For example, you might define a reply which includes fields for a sender's name, department and telephone number. Each time this template is applied to messages, the fields are replaced with the Active Directory content for these fields, for the sender.

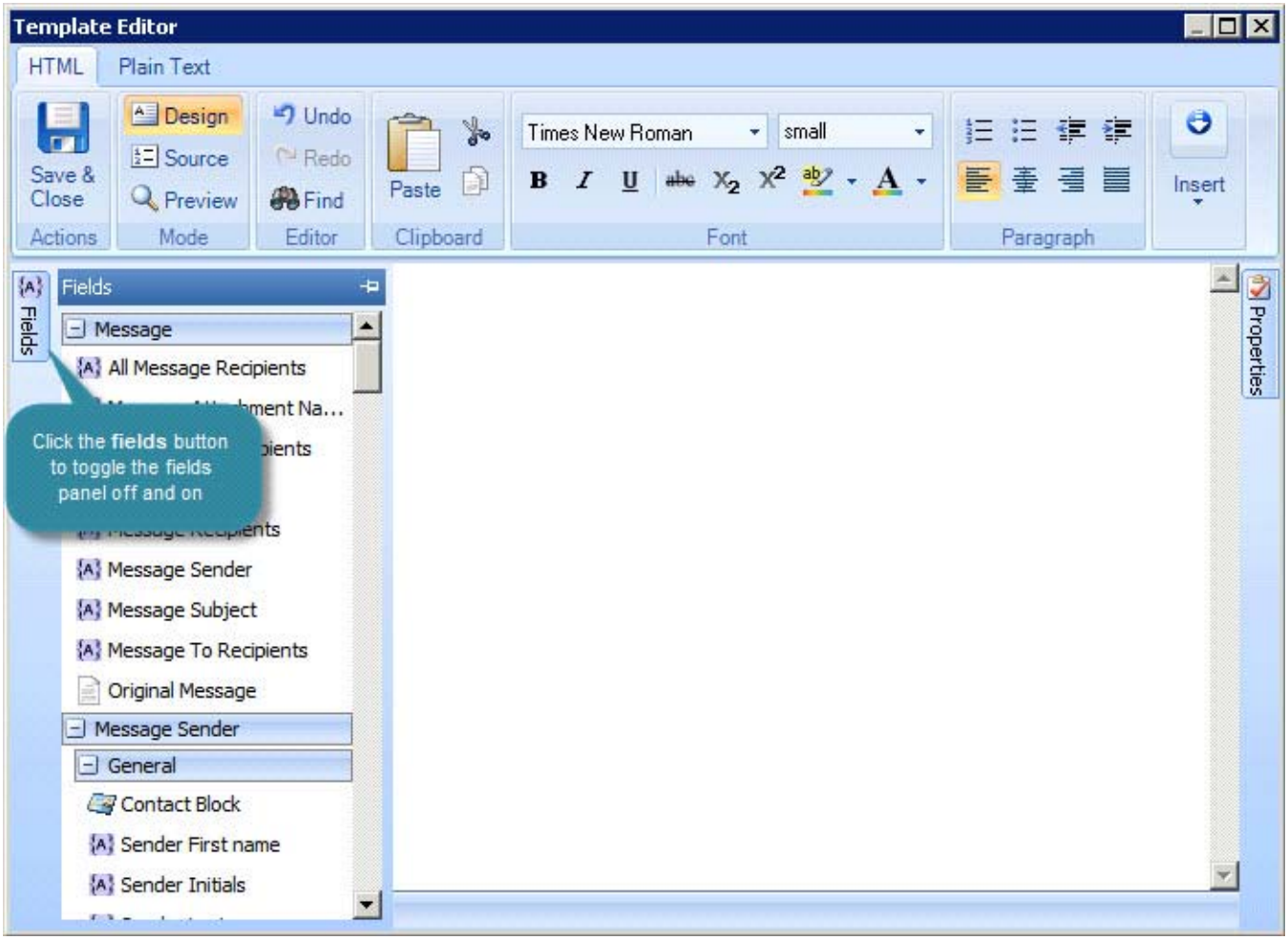
Fields can be inserted into both HTML and plain text template types. This section contains useful information for working with fields, including:

- Working with the fields panel [see page 199]
- Working with fields [see page 200]
- Available fields [see page 201]

Fields can also be used when defining auto response policy settings [see page 78].

Working With the Fields Panel

When not in use, the fields panel is hidden, to avoid cluttering editing space in the template editor [see page 184]. To activate this panel, click the fields option on the top, left-hand side of the template editor:



Scroll down the list to view fields, which are organized into related groups, namely:

- Message [see page 201]
- Message sender [see page 203]
- Message recipient [see page 209]
- Dynamic content [see page 215]
- Server [see page 224]
- General [see page 224]

To insert a field, simply double click the required entry in the panel. The field is inserted and the fields panel closes automatically, so you can start working with the field [see page 200] in the editor. If you do not wish to insert a field, click the fields button to close the panel.

Techniques for Working with Fields

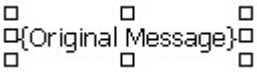
Using Spaces Between Fields

The placement of content will be made exactly as displayed in the editor. For example, if you enter three blank lines between your automatic reply content and an original message field , there will be three blank links at the end of your automatic reply, followed by the original message.

Copying and Pasting Original Message Fields

You can copy and paste fields to new positions within the template - care should be taken to ensure you copy/paste the entire field rather than just the text element. When you click on a field, it behaves like a table cell. For a correct selection, you should see the borders of the cell clearly marked. For example:

...or



Available Fields

This section summarizes all fields that can be used when defining templates in Exclaimer Auto Responder:

- Message fields [see page 201]
- Message sender fields [see page 202]
- Message recipient fields [see page 209]
- Dynamic content fields [see page 215]
- Server fields [see page 224]
- General fields [see page 224]

Message Fields

Fields in the message group are summarized below:

Field	Inserts...
Message Attachment Name(s)	The name of any attached files with the message.
Message CC Recipients	Any email addresses specified in the CC field.
Message Date	The message sent or received date.
Message Recipients	The email address of all recipients of the email (i.e. those specified in the To field and the CC field).
Message Sender	The email address of the message sender.
Message Subject	The content of the message subject line.
Message To Recipients	The email address of all recipients entered in the To field.
Original Message	The original message content. Use this field to place the original email message before or after automatic reply content [see page 191].
Recipients Matching Condition	All recipients of the original message (including those who were blind copied) who matched the condition.

Message Sender Fields

This section summarizes message sender fields which can be used when defining templates in Exclaimer Auto Responder:

- Message sender general fields [see page 203] _ [see page 203]
- Message sender address fields [see page 204] _ [see page 204]
- Message sender telephones fields [see page 205] _ [see page 205]
- Message sender organization fields [see page 206] _ [see page 206]
- Message sender Exchange Advanced fields [see page 207] _ [see page 207]
- AD pictures fields [see page 207]
- Other AD fields [see page 208]

Message Sender - General Fields

Fields in the message sender - general section are summarized below:

Field	Inserts...
Contact Block	A block of contact information for the sender in tabular form. Use this option to select fields to be grouped in a table as a standard contact block. This is a good way to add signature-type details to an automatic reply, since you can suppress fields if they are blank and so avoid blank lines in a signature (or any other block of fields). For further information and an example see page 235.
Sender First Name	The first name of the message sender.
Sender Initials	Initials for the message sender.
Sender Last name	The last name of the message sender.
Sender Display name	Display name for the message sender.
Sender Description	Description information for the sender.
Sender Office	Office information for the sender.
Sender Telephone Number	Telephone number for the sender.
Sender Other Telephone Number	Other telephone number for the sender.
Sender E-mail	E-mail address for the sender.
E-mail (as hyperlink)	E-mail address presented as a hyperlink, for the sender.
Sender Web Page	Web page address for the sender.
Web Page (as hyperlink)	Web page address for the sender, presented as a hyperlink.
Sender Other Web Page	Alternative web page for the sender.

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **office** field to indicate the office location in which a user is based, whilst another may use this field for something completely different.

Message Sender - Address Fields

Fields in the message sender - address section are summarized below:

Field	Inserts...
Address Block	A block of address information for the sender in tabular form. Includes street, city, state/province and zip/postal code. View example.
Sender Street	Street information for the sender.
Sender P.O. Box	P.O. Box information for the sender.
Sender City	City information for the sender.
Sender State/Province	State/province information for the sender.
Sender Zip/Postal Code	Zip/postal code information for the sender.
Sender Country/Region	Country/region information for the sender.
Sender Country/Region (2 letters)	Two letter country abbreviation for the sender (e.g. UK).

This information is taken from the Active Directory, therefore content may vary from one organization to another. For example, one organization may use the **P.O. Box** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Sender - Telephone Fields

Fields in the message sender - telephone section are summarized below:

Field	Inserts...
Sender Home	Home telephone number for the sender.
Sender Other Home	Other home telephone number for the sender.
Sender Pager	Pager number for the sender.
Sender Other Pager	Other pager number for the sender.
Sender Mobile	Mobile telephone number for the sender.
Sender Other Mobile	Other mobile number for the sender.
Sender Fax	Fax number for the sender.
Sender Other Fax	Other fax number for the sender.
Sender IP Phone	IP phone number for the sender.
Sender Other IP Phone	Other IP phone number for the sender.
Sender Notes	Notes for the sender.

This information is taken from the Active Directory, therefore content may vary from one organization to another. For example, one organization may use the **notes** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Sender - Organization Fields

Fields in the message sender - organization section are summarized below:

Field	Inserts...
Sender Title	The message sender's job title.
Sender Department	The department in which the message sender works.
Sender Company	The company for whom the message sender works.
Sender Manager Display Name	The name of the message sender's manager.
Sender Manager E-mail	The email address of the message sender's manager.
Sender Manager E-mail (as hyperlink)	The email address of the message sender's manager, presented as a hyperlink.

This information is taken from the Active Directory, therefore content may vary from one organization to another. For example, one organization may use the **department** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Sender - Exchange Advanced Fields

These fields are a set of standard fields added by Exchange, in which administrators can place any data that they require. There will be fields named Extension Attribute X, where X is a number between 1 and 15.

Message Sender - AD Pictures Fields

Fields in the AD Pictures section are summarized below:

Field	Inserts...
Sender JPEG Photo	Insert JPEG photo of the sender.
Sender Photo	Insert other photo of the sender.
Sender Thumbnail Logo	Insert thumbnail logo associated with the sender.
Sender Thumbnail Photo	Insert thumbnail photo associated with the sender.

Although the Active Directory includes fields for pictures, there is no in-built, straightforward way to add pictures to it. The Exclaimer AD Pictures application allows you to create and manage images for all objects in your Active Directory - please contact us if you would like further information.

Message Sender - Other AD Fields

Fields in the other AD fields section are summarized below:

Field	Inserts...
Sender Home Address	Insert the sender's home address.
Sender Personal Title	Insert the sender's personal title.
Postal Address	Insert the sender's postal address.
Sender AD field	Insert details from the Sender AD field (this can be used to access data in the Active Directory for which no specific field exists in Auto Responder).

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **postal address** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Recipient Fields

This section summarizes message recipient fields which can be used when defining templates in Exclaimer Auto Responder:

- Message recipient - general fields [see page 210]
- Message recipient - address fields [see page 211]
- Message recipient - telephones fields [see page 212]
- Message recipient - organization fields [see page 213]
- Message recipient - exchange advanced fields [see page 213]
- Message recipient - AD pictures fields [see page 214]
- Message recipient - other AD fields [see page 214]

Message Recipient - General Fields

Fields in the message recipient - general section are summarized below:

Field	Inserts...
Recipient First Name	The first name of the message recipient.
Recipient Initials	Initials for the message recipient.
Recipient Last name	The last name of the message recipient.
Recipient Display name	Display name for the message recipient.
Recipient Description	Description information for the recipient.
Recipient Office	Office information for the recipient.
Recipient Telephone Number	Telephone number for the recipient.
Recipient Other Telephone Number	Other telephone number for the recipient.
Recipient E-mail	E-mail address for the recipient.
Recipient Web Page	Web page address for the recipient.
Recipient Other Web Page	Alternative web page for the recipient.

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **office** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Recipient - Address Fields

Fields in the message recipient - address section are summarized below:

Field	Inserts...
Recipient Street	Street information for the recipient.
Recipient P.O. Box	P.O. Box information for the recipient.
Recipient City	City information for the recipient.
Recipient State/Province	State/province information for the recipient.
Recipient Zip/Postal Code	Zip/postal code information for the recipient.
Recipient Country/Region (2 letters)	Two letter country abbreviation for the recipient (e.g. UK).

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **P.O Box** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Recipient - Telephones Fields

Fields in the message recipient - telephone section are summarized below:

Field	Inserts...
Recipient Home	Home telephone number for the recipient.
Recipient Other Home	Other home telephone number for the recipient.
Recipient Pager	Pager number for the recipient.
Recipient Other Pager	Other pager number for the recipient.
Recipient Mobile	Mobile telephone number for the recipient.
Recipient Other Mobile	Other mobile number for the recipient.
Recipient Fax	Fax number for the recipient.
Recipient Other Fax	Other fax number for the recipient.
Recipient IP Phone	IP phone number for the recipient.
Recipient Other IP Phone	Other IP phone number for the recipient.
Recipient Notes	Notes for the recipient.

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **notes** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Recipient - Organization Fields

Fields in the message recipient - organization section are summarized below:

Field	Inserts...
Recipient Title	The message recipient's job title.
Recipient Department	The department in which the message recipient works.
Recipient Company	The company for whom the message recipient works.
Recipient Manager Display Name	The name of the message recipient's manager.
Recipient Manager E-mail	The email address of the message recipient's manager.

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **department** field to indicate a genuine box number, whilst another may use this field for something completely different.

Message Recipient - Exchange Advanced Fields

These fields are a set of standard fields added by Exchange, in which administrators can place any data that they require. There will be fields named Extension Attribute X, where X is a number between 1 and 15.

Message Recipient - AD Pictures Fields

Fields in the AD Pictures section are summarized below:

Field	Inserts...
Recipient JPEG Photo	Insert JPEG photo of the recipient.
Recipient Photo	Insert other photo of the recipient.
Recipient Thumbnail Logo	Insert thumbnail logo associated with the recipient.
Recipient Thumbnail Photo	Insert thumbnail photo associated with the recipient.

Although the Active Directory includes fields for pictures, there is no in-built, straightforward way to add pictures to it. The Exclaimer AD Pictures application allows you to create and manage images for all objects in your Active Directory - please contact us if you would like further information.

Message Recipient - Other AD Fields

Fields in the other AD fields section are summarized below:

Field	Inserts...
Recipient Home Address	Insert the recipient's home address.
Recipient Personal Title	Insert the recipient's personal title.
Postal Address	Insert the recipient's postal address.
Recipient AD Field	Insert details from the Recipient AD field (this can be used to access data in the Active Directory for which no specific field exists in Auto Responder).

This information is taken from the Active Directory; therefore content may vary from one organization to another. For example, one organization may use the **postal address** field to indicate a genuine box number, whilst another may use this field for something completely different.

Dynamic Content Fields

This section summarizes dynamic content fields which can be used when defining templates in Exclaimer Auto Responder:

- Rotating banner ad [see page 218]
- Custom image [see page 217]
- Custom hyperlink [see page 216]
- Content from file [see page 215]
- RSS feed [see page 219]
- Composite field [see page 220]
- Smart tables [see page 221]

Content from File

The content from file field is used to insert content from an external document, by specifying a location for the required document.

This is useful (for example) if you need to use content for an automatic reply that is constantly being updated - rather than adding text directly into the template editor each time there is a change, simply specify a location to the original file and the latest content will always be included. The file location specified must be accessible to the user NETWORK SERVICE.

To use content from an existing file in a template, follow the steps below:

1. Use the fields panel to insert a content from file field.
2. Select the newly inserted field and check the properties pane - a property named file location is shown (view example).
3. Click the browse button to open the file location window (view example).
4. Click browse to navigate drives and folders (view example).
5. Select the required file and click open to select the file.

> Remember that you can switch to **preview** mode (from the template editor toolbar [see page 188]) to see the effect of any dynamic fields you have inserted.

Custom Hyperlink

A custom hyperlink can be used to insert a standard hyperlink (i.e. a URL for a web page), and any other kind of link (for example, a mailto email link). Additionally, it has the option to include other Active Directory fields.

This means that you can create a custom hyperlink and insert (for example) the message sender > web page field to insert a link to the sender's own web page in an automatic reply. To insert a custom hyperlink and specify a field within it, follow the steps below:

1. Use the fields panel to insert a custom hyperlink field.
2. Select the newly inserted field and check the properties pane - properties for the hyperlink are shown (view example).
3. Set properties as follows:

Action	Summary
Address	Click the browse button to the right of the address field, to open the address window (view example). Click insert to navigate available fields and select the required entry (view example).
Hover Text	Enter text to be displayed when a user hovers the cursor over the link.
Text to Display	Enter text that users click to activate the link) (view example).

Remember that you can switch to **preview** mode (from the template editor toolbar [see page 188]) to see the effect of any dynamic fields you have inserted.

Custom Image

The custom image field allows you to insert an image and use it as a trigger for a hyperlink (view example). You can specify an image from a specific file location, or from an Active Directory field. To do this, follow the steps below:

1. Use the fields panel to insert a custom image field. The image location window is displayed.
2. Click browse to navigate local and network drives and select the required image.
3. Having selected the image, click OK to close the image location window and return to the template editor.
4. Select the newly inserted image.
5. Check the properties pane - properties for the image are shown (view example).
6. Set properties as follows:

Action	Summary
Address	Use this option to apply a hyperlink to the image. Click the browse button to the right of the address field, to open the address window. Type the required URL into the address field (i.e. the web address that should be displayed when a user clicks the image in the message (view example). Alternatively, click insert to navigate available fields and select an Active Directory field as the link target (for example, you might wish to use the message sender's or recipient's web page).
Hover Text	Enter text to be displayed when a user hovers the cursor over the image.
Alt Text	Enter text to be displayed if images cannot be displayed.
Image Location	Use this property as a way to change the custom image. Click the browse button to the right of the image location field, to open the image location window. Click browse to navigate drives and folders to specify an image location. Alternatively, click insert to navigate available fields and select an Active Directory field to insert as the image (for example, you might wish to use the message sender's or recipient's thumbnail photo).

Remember that you can switch to **preview** mode (from the template editor toolbar [see page 188]) to see the effect of any dynamic fields you have inserted.

Rotating Banner Ad

The rotating banner ad field allows you to specify multiple images in a given folder location so, when displayed in messages, the image changes (rotating through images in the given folder).Images can be associated with a (single) hyperlink so the given web address is displayed when an image is clicked. Image rotation can be set to either random or sequential.

To add a rotating banner ad, follow the steps below:

1. Use the fields panel to insert a rotating banner ad field. The folder location window is displayed.
2. Click browse to navigate local and network drives and select the required folder (i.e. the folder that contains images to be used).
3. Having selected the required folder, click OK to close the folder location window and return to the template editor.
4. Select the newly inserted field and check the properties pane - properties for the field are shown (view example).
5. Select the drop-down list to the right of the banner chooser field.
6. Scroll down to the sequence section and choose whether to display images in sequence, or randomly (view example).
7. Set remaining properties as follows:

Action	Summary
Address	Use this option to apply a hyperlink to banner images. Click the browse button to open the address window and type the required URL into the address field (i.e. the web address that should be displayed when a user clicks an image in the message. Alternatively, click the insert button to navigate available fields and select an Active Directory field as the link target (for example, you might wish to use the message sender's web page).
Alt Text	Enter text to be displayed if images cannot be displayed.
Filter	If required, you can use wildcards so that only certain images are used (for example, you might wish to use a series of images which start with 'sales' and would therefore specify 'sales*.*' or you might only wish to use JPEG images and therefore specify '*.JPG'.
Folder Location	Click the browse button to open the folder location window (view example). Click browse to navigate drives and folders to specify a folder location. Alternatively, click insert to navigate available fields and select an Active Directory field to insert as the location.
Hover Text	Enter text to be displayed when a user hovers the cursor over a rotating banner ad image

RSS Feed

Use the RSS feed option to insert an RSS feed into email messages (view example). To insert a feed, follow the steps below:

1. Use the fields panel to insert an RSS feed field. A content window is displayed, which is similar to the template editor but it is only used to add RSS fields.
2. In the content window, click the fields button to open the fields panel. The RSS feed field is a composite field [see page 220], which means it is comprised of multiple fields; by default, these fields are RSS Title and RSS Description, however you can add additional elements using fields shown here (view example).
3. Add any RSS fields that you wish to include in the template.
4. Click OK to return to the template editor.
5. Select the newly inserted field and check the properties pane - properties for the feed are shown (view example).
6. Set properties as follows:

Action	Summary
Content	The RSS feed field is a composite field [see page 220], which means it is comprised of multiple fields. By default, these fields are RSS Title and RSS Description, however you can click the browse button to open the composite field editor and amend these (if required).
RSS Channel	Some organizations have feeds with multiple channels - for example, one channel for news and another for announcements. Use this option if a specific channel selection is required.
RSS Item	Choose whether to display a random feed entry, or a sequential number. Use the drop-down list and scroll down to the sequencers section to change this setting.
RSS URL	Enter required URL for the feed.

Remember that you can switch to **preview** mode (from the template editor toolbar [see page 188]) to see the effect of any dynamic fields you have inserted.

Composite Field

A composite field is used as a container for multiple fields that need to be used together. For example, you might define a composite field which contains department, company and sender's web page, or you might define a composite field to include the number and size of message attachments. A composite field might contain just fields, but it can also contain text.

To define a composite field, follow the steps below:

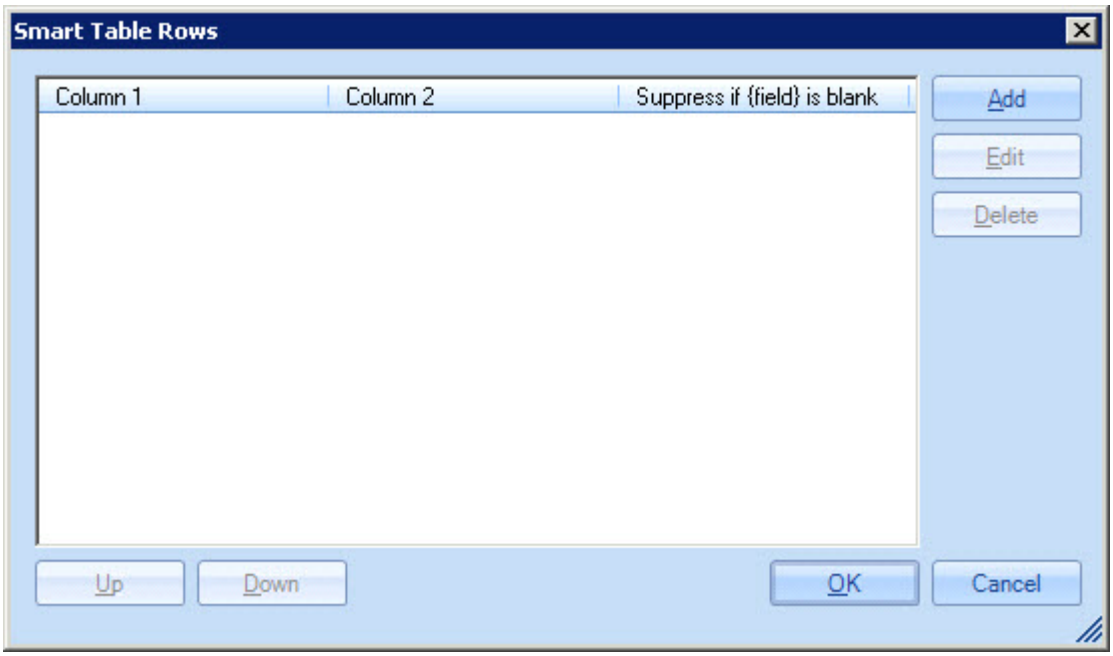
1. Use the fields panel to insert a composite field. The content window is very similar to the template editor, but it is only used to add fields to the composite.
2. In the content window, click the fields button to open the fields panel.
3. Add any fields that you wish to make up the composite field. As with any other fields, you can set properties [see page 226] to control behavior and formatting (view example).
4. Click OK to return to the template editor.
5. If required, select the newly inserted composite field and view/adjust properties.

> Remember that you can switch to **preview** mode (from the template editor toolbar [see page 188]) to see the effect of any dynamic fields you have inserted.

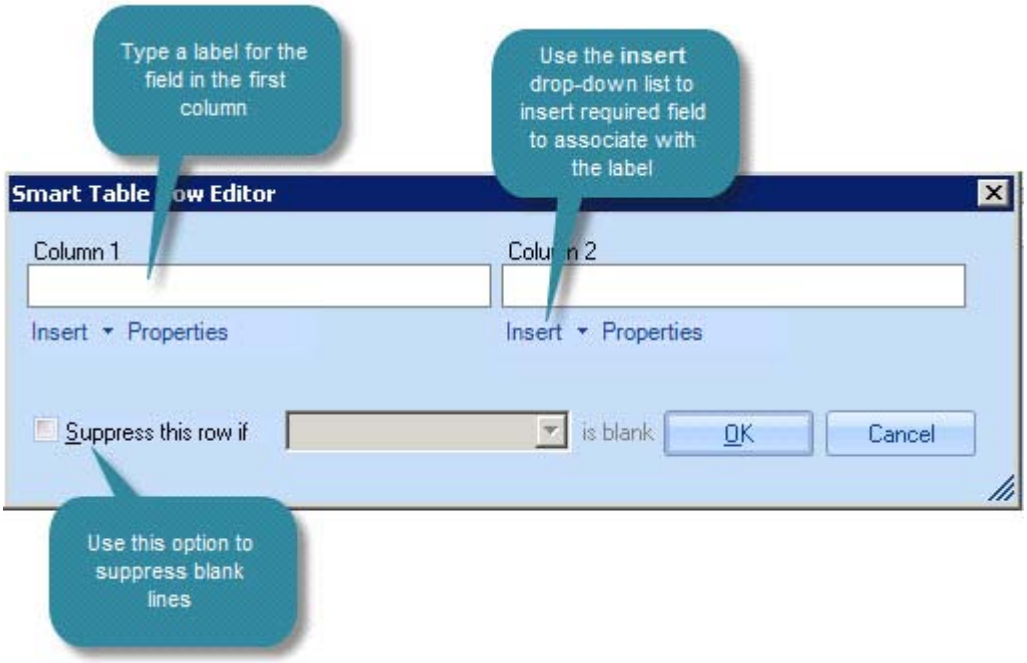
Smart Tables

The smart tables field can be used to insert a table and specify content / attributes using straightforward data entry fields. This is a quick and easy way to insert a table and include Active Directory fields (or other content) at the same time; the alternative would be to insert a standard HTML table [see page 195] and add fields or other content manually.

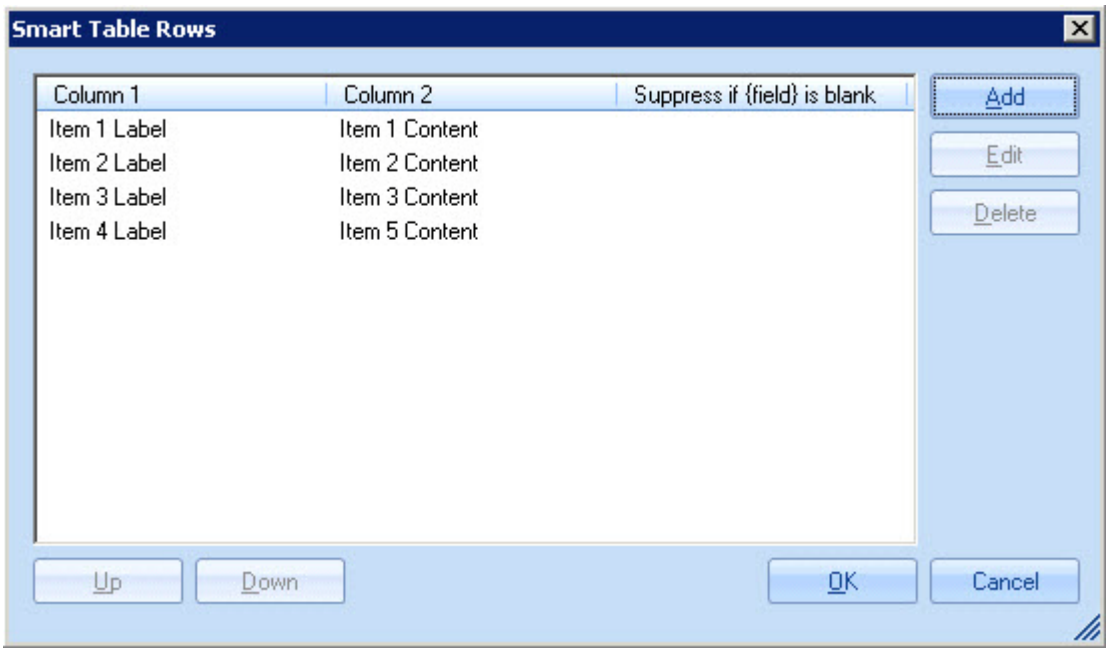
Having selected the smart tables field, the smart table rows window is displayed:



From here, click add to start adding rows to the table. The smart table row editor allows you to define content for each column in the row - you can add text or fields, as required. If you are adding a field, you can suppress this row if no Active Directory information is found for the field when the policy is processed:



Continue to add as many rows as required:



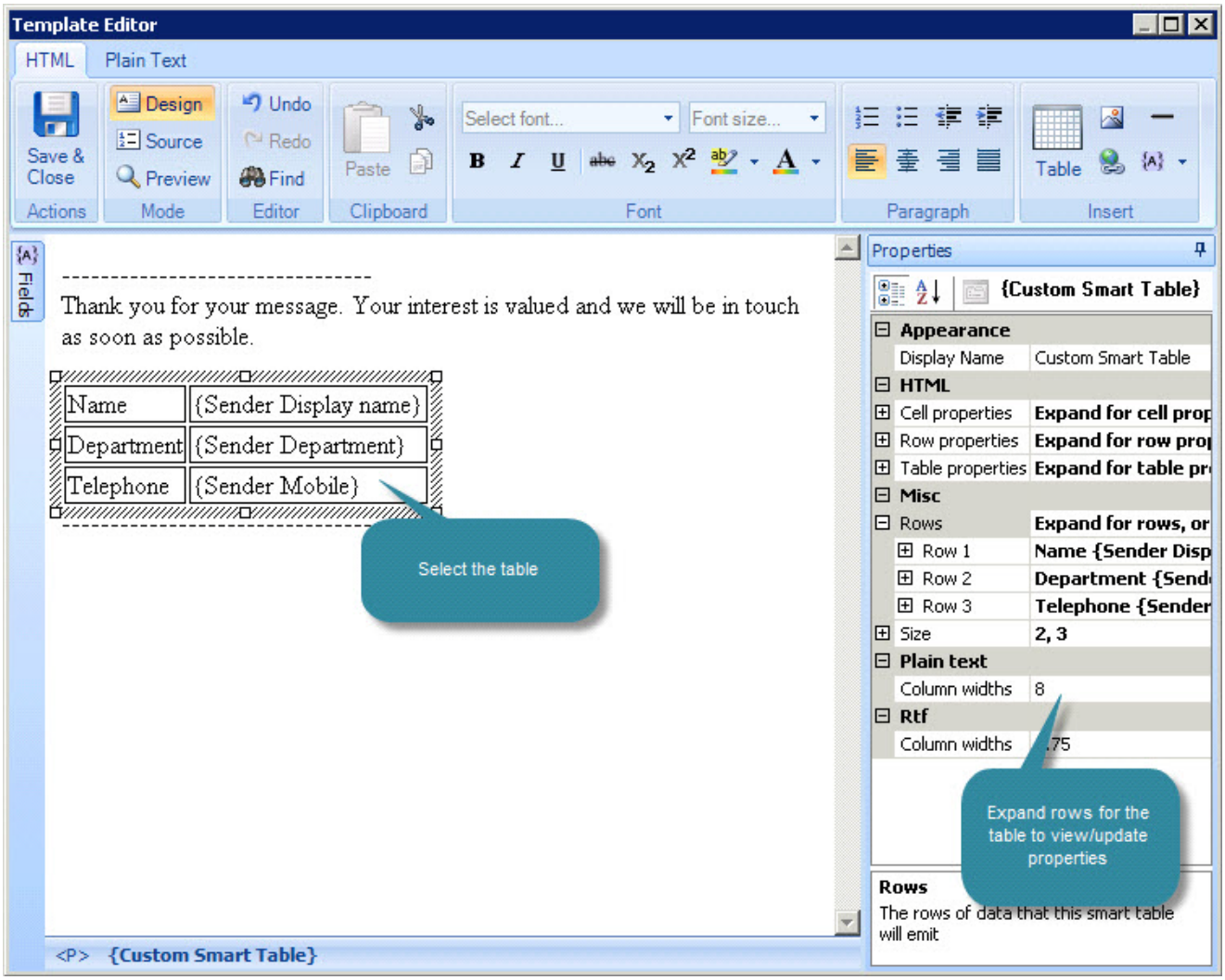
If required, you can select a row and use up / down options to adjust the sequence. You can also edit and delete existing rows. Once all rows have been added, click OK to insert the table into the template:

Item 1 Label	Item 1 Content
Item 2 Label	Item 2 Content
Item 3 Label	Item 3 Content
Item 4 Label	Item 5 Content

Updating an existing smart table

To update an existing smart table in a template, simply select and double-click the table.

Alternatively, select the entire table and expand the misc section in the properties pane. From here, select the browse - ... - button to the right of the cell properties entry. The smart table rows window is displayed so you can add, edit or remove rows as required:



Server Fields

Fields in the server fields section are summarized below:

Field	Inserts...
Server Distinguished Name	Distinguished name information for the mail server (for example: CN=HELPDC,OU=Domain Controllers,DC=network26,DC=local)
Server IP Address	IP address details for the mail server (for example: fe80::e5ce:af42:688c:d2d8%10 192.168.26.1)
Server Locale	Locale information for the mail server (for example: en-US)
Server NETBIOS Name	The NETBIOS name for the mail server (for example: HelpDC)
Server Qualified Domain	Qualified domain information for the mail server (for example: HelpDC.network26.local)

General Fields

Fields in the general fields section are summarized below:

Field	Inserts...
Current Date	The current date (which may not necessarily be the same as the message sent date)

Properties

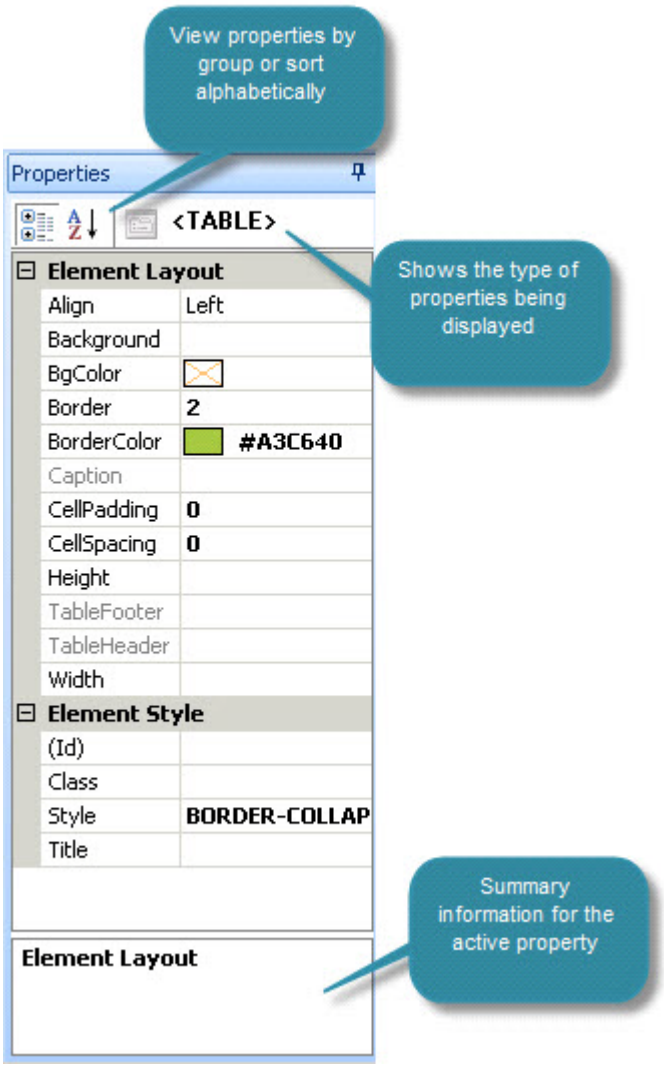
Properties are used to format and control template content - almost every piece of content added to a template will have properties associated with it. For example, a section of text will have various font properties, a table cell will have border and background color properties and a hyperlink will have URL and target properties.

Properties are used in both HTML and plain text templates. This section contains useful information for working with properties, including:

- Working with the properties pane [see page 226]
- Examples of properties in use [see page 227]

Working With the Properties Pane

The properties pane updates to reflect the current selection in the template editor:



The title at the top of the properties panel shows the type of properties displayed - i.e. the nature of the selected item of content. In the above example, a table was selected in the HTML editor, so the title of the property pane is displayed as <table>.

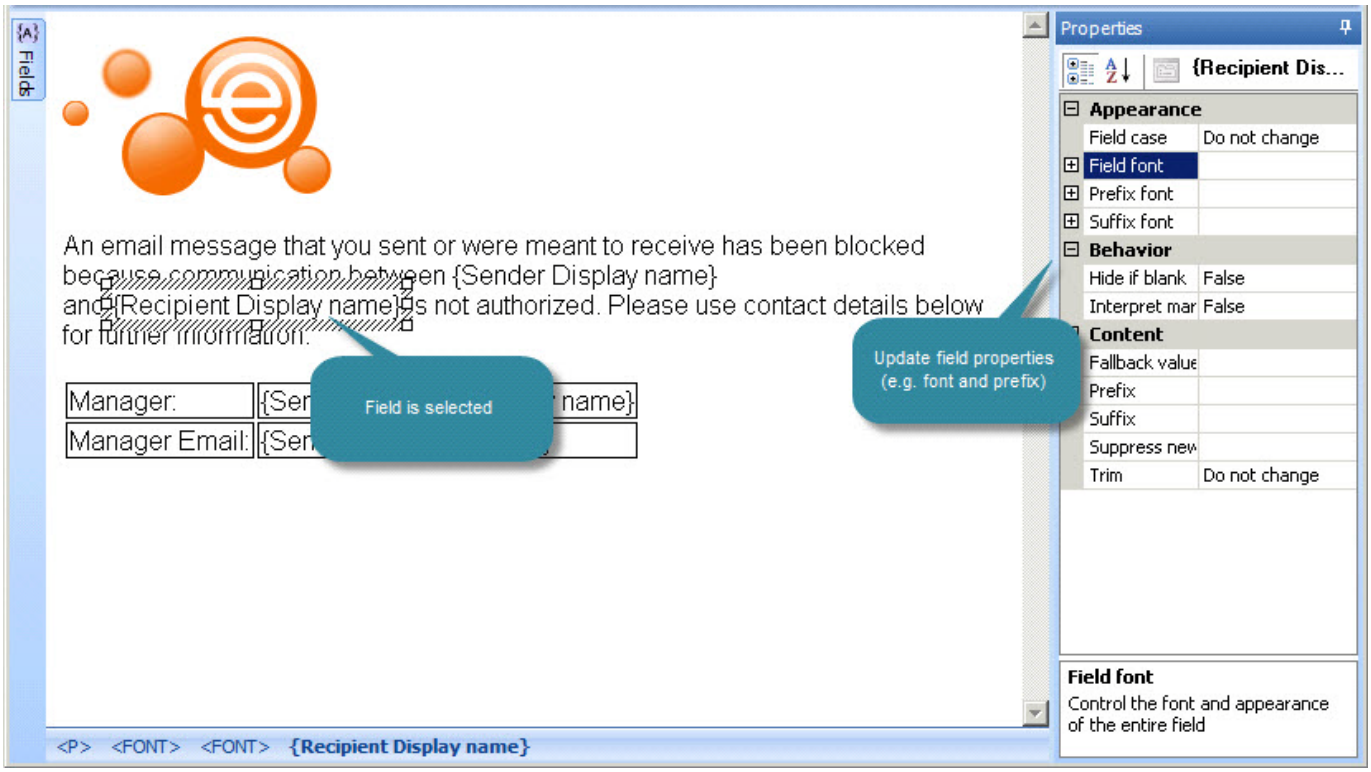
Many properties are associated with drop-down lists so you can select a pre-defined value, whilst others require direct input. At the bottom of the properties pane, a small information area displays summary text for the currently selected property.

Remember - almost all items of content entered into the template editor will have properties associated with them. If you aren't sure how to change something, select it and check available properties.

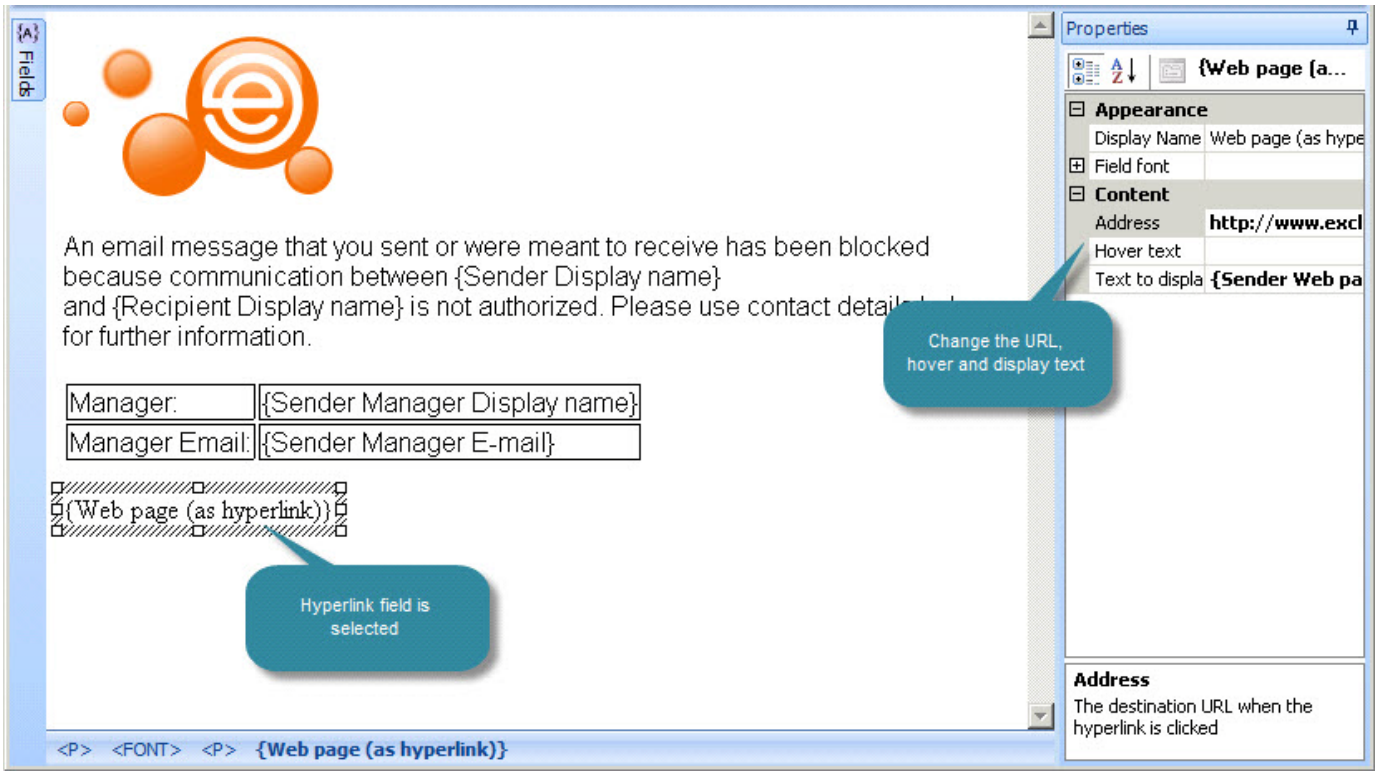
Examples of Properties in Use

The following examples show how the properties pane [see page 226] updates to reflect selected content in the template editor:

Field Properties



Hyperlink Properties



Text Properties

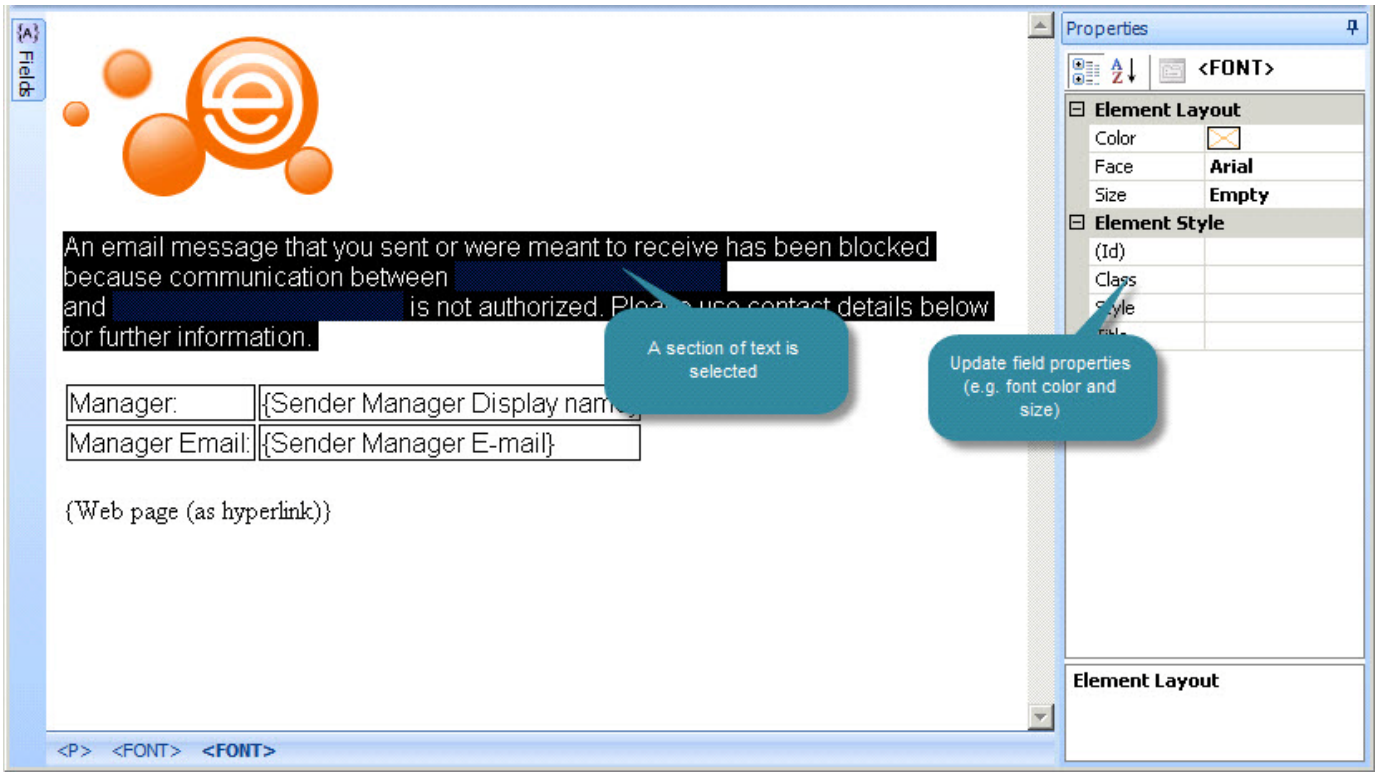
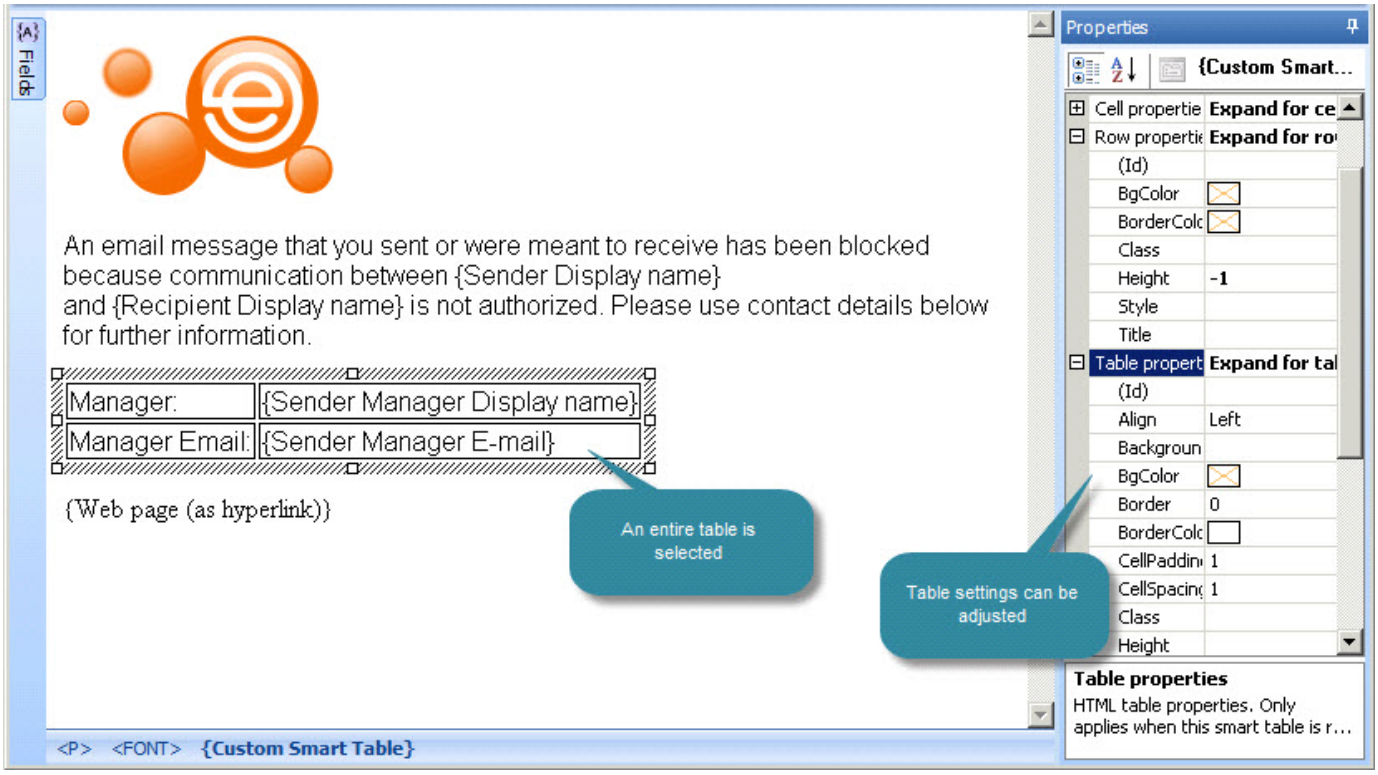


Table Properties



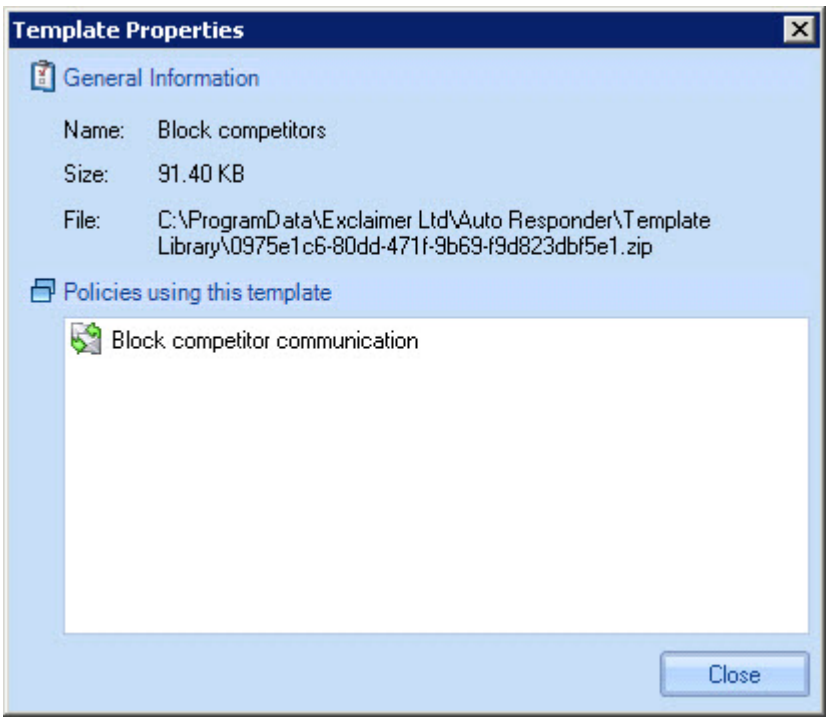
How To...

This section contains instructions for completing a selection of common tasks with templates using Exclaimer Auto Responder, including:

- How can I tell which policies are using a specific template? [see page 230]
- How do I include the original message in an automatic reply? [see page 231]
- How do I set the font for text in an automatic reply? [see page 232]
- How do I suppress blank lines if fields are not populated? [see page 233]
- How do I create a contact block? [see page 235]
- How do I insert a banner image at the start of automatic replies? [see page 239]

How can I Tell which Policies are Using a Specific Template?

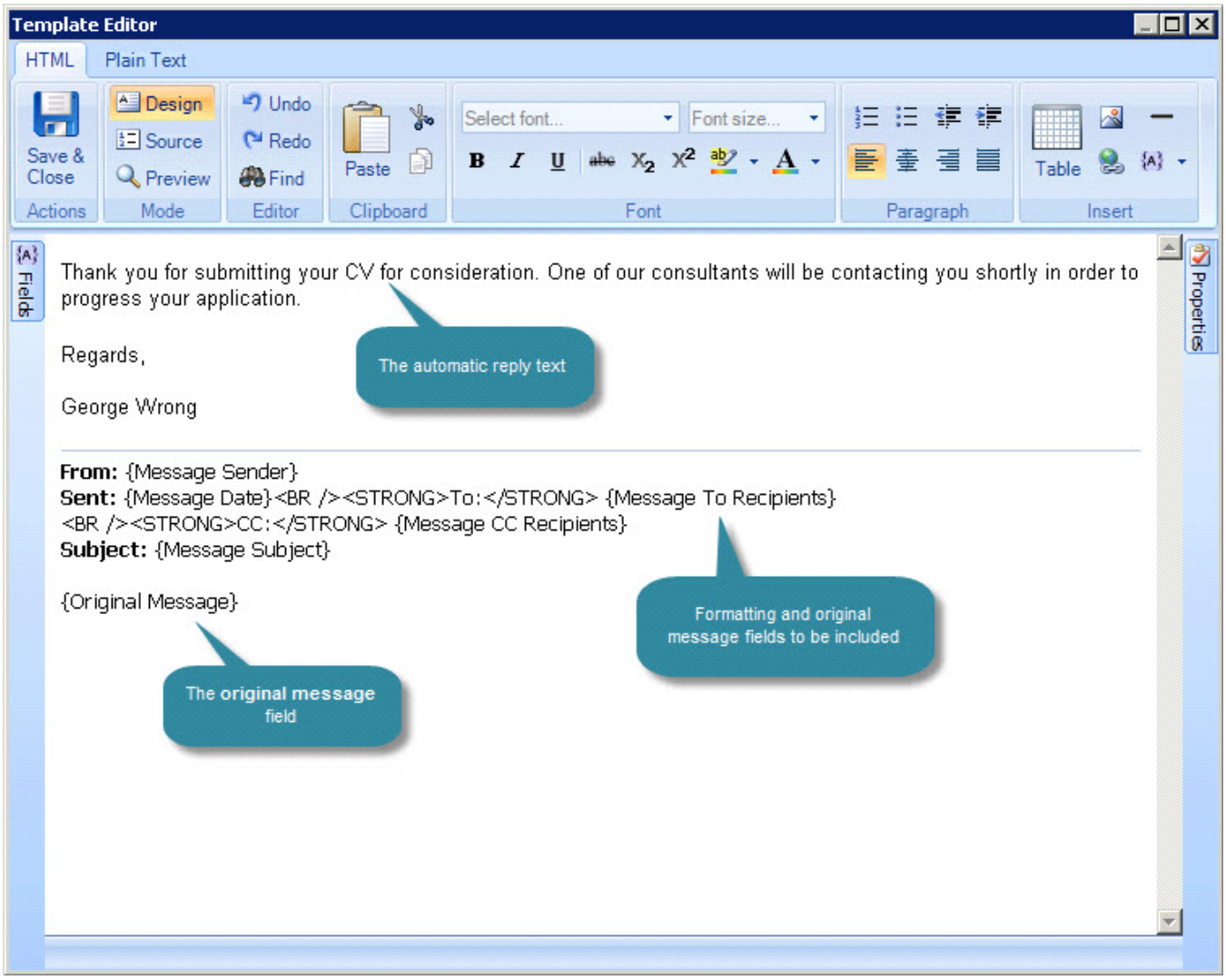
Each template is associated with a properties window, which includes a list of any policies which are using the template:



The properties option is available from the template library toolbar and from the right-click menu.

How do I Include the Original Message in an Automatic Reply?

If you wish to include the original email message in an automatic reply, you can add an original message field from the fields panel [see page 199]:



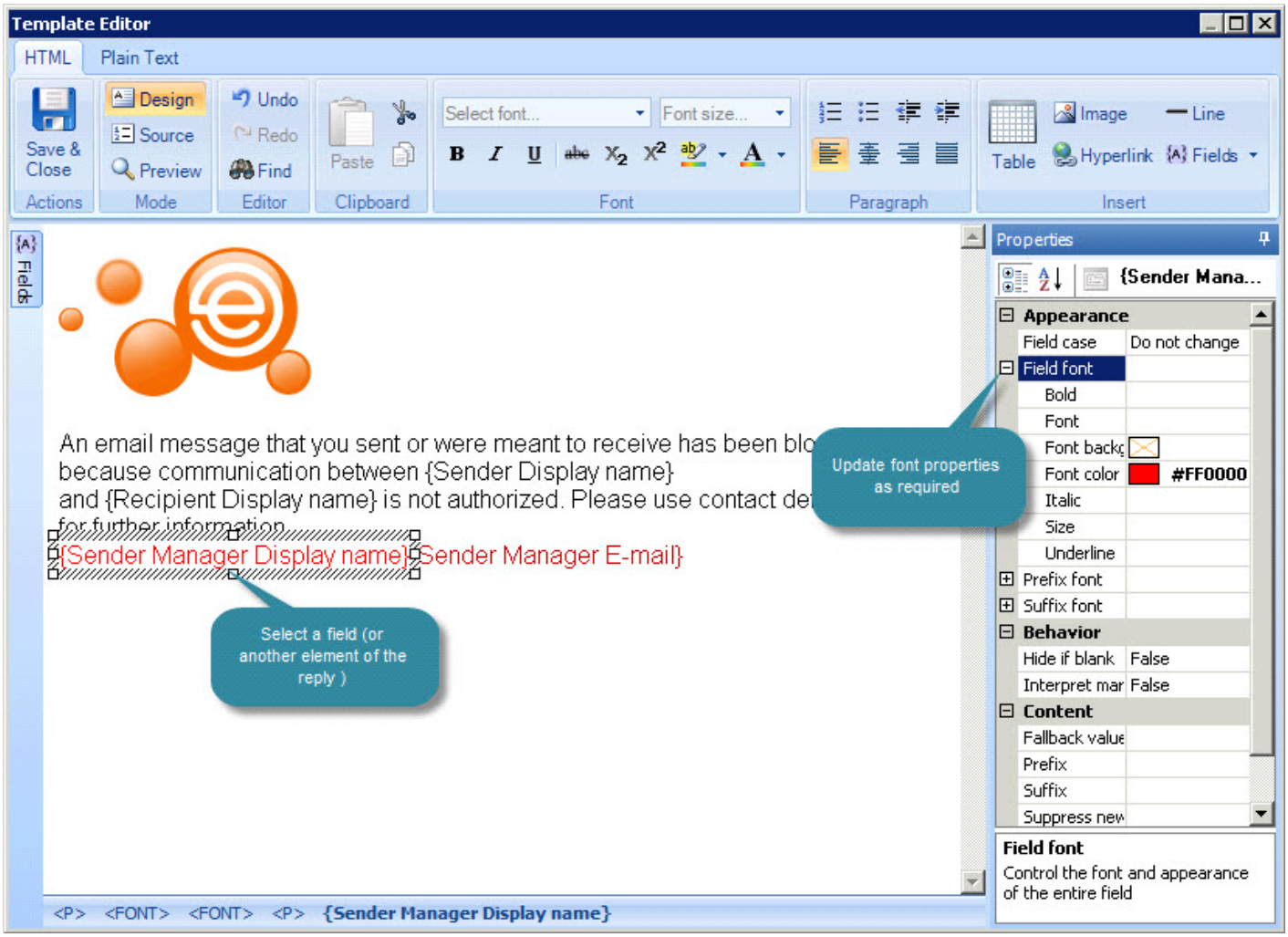
The original message field should be placed according to where you want the original message to be displayed, relative to the automatic reply. For example, place it below automatic reply text to show the original message after the automatic reply content. As well as the body of the original message, you can also insert other fields relating to the message (for example, recipients, date sent, etc) as shown in the example above.

If required, you can choose to attach a copy of the original message to an automatic reply. To do this, select the **attach original message** option on the auto response tab [see page 78] for the required policy.

For further information about working with the original message field see the placement of content section on page 194.

How do I Set the Font for Text in an Automatic Reply?

To set the font (and any other formatting attributes) for field items in a template, select the required field and use field font properties in the properties panel (shown below). You can also apply formatting via the template editor toolbar [see page 185]:



How do I Suppress Blank Lines if Fields are not Populated?

When using fields in templates, it is often useful to suppress an item if there is no data in the Active Directory to populate the field for a given user. There are two ways to suppress blank lines - use a contact block [see page 233] or use a field prefix [see page 234].

Use a Contact Block

A contact block is a pre-defined set of fields, presented in tabular form. For example:

Tel:	{Telephone number}
Fax:	{Fax}
Mobile:	{Mobile}
Email:	{E-mail (as hyperlink)}

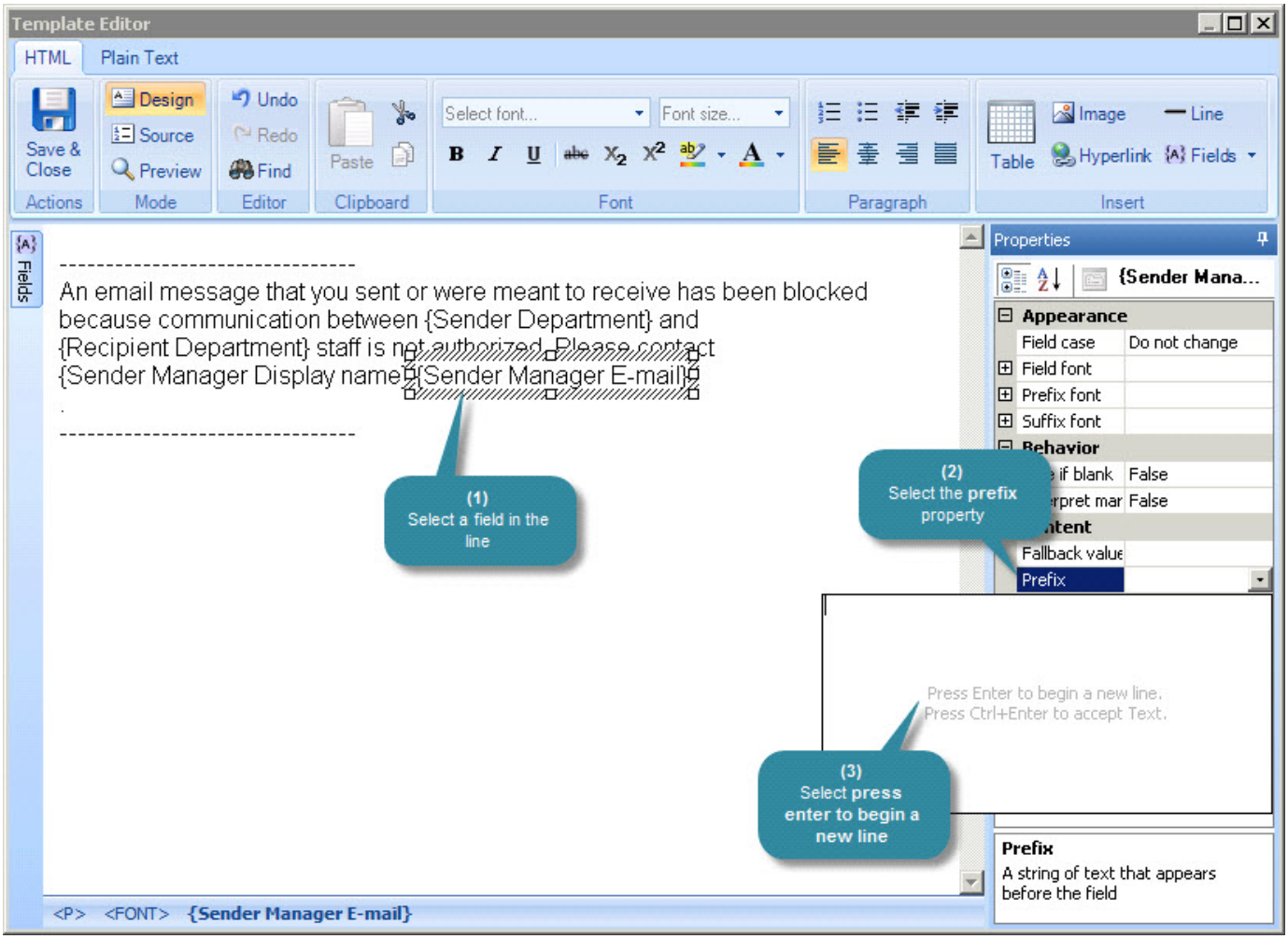
...produces:

Tel:	+44 (0) 1252 987 456
Fax:	+44 (0) 1252 987 456
Mobile:	+44 (0) 7733 102345
Email:	kareng@greenorg.net

When a contact block is used, rows are not displayed if Active Directory data is not present. See how do I create a contact block? on page 235 for further information.

Use a Field Prefix

An alternative approach is to place all required fields on a single line, but use the prefix property to insert a carriage return before each one (shown below):



How do I Create a Contact Block?

Example of a contact block

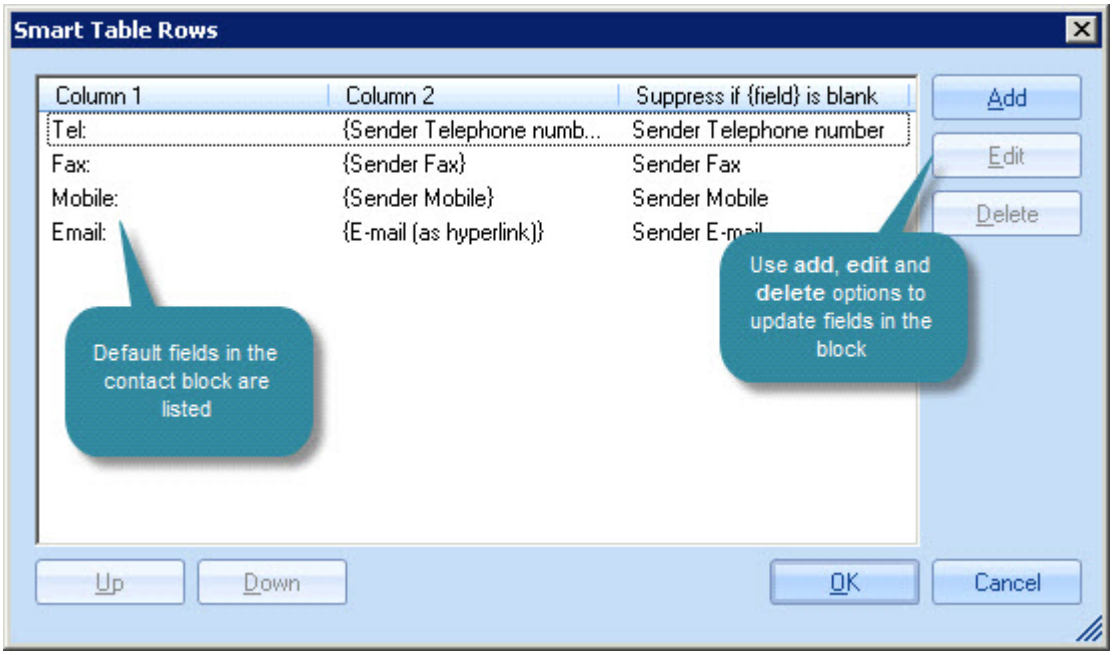
Tel:	{Telephone number}
Fax:	{Fax}
Mobile:	{Mobile}
Email:	{E-mail (as hyperlink)}

...produces:

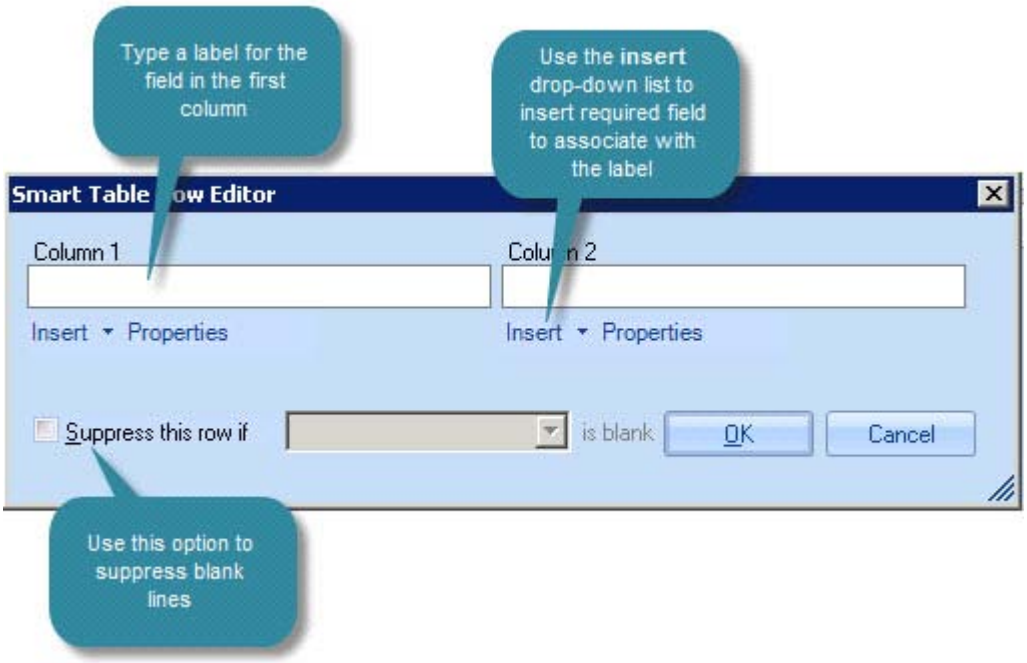
Tel: +44 (0) 1252 987 456
Fax: +44 (0) 1252 987 456
Mobile: +44 (0) 7733 102345
Email: kareng@greenorg.net

How it works

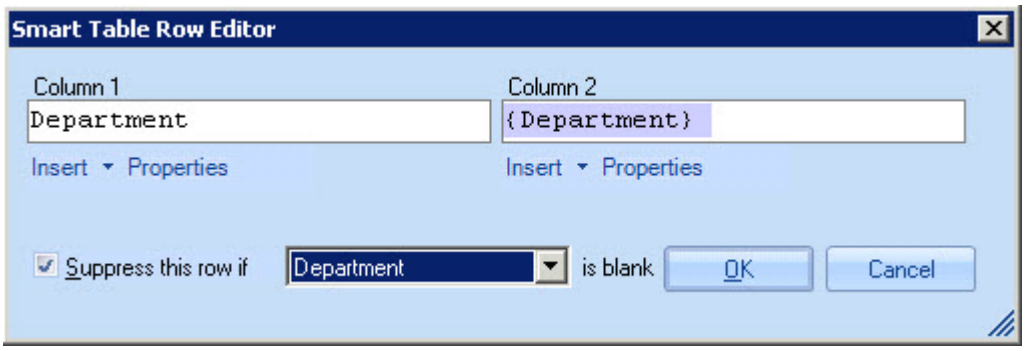
When the contact block field is selected, the auto table rows window is displayed. Use this window to specify which fields to include in the table:



Click add to add a new row to the contact block table:



Contact blocks can be arranged as required but a typical layout has a field label in the left column and the corresponding field in the right column - for example:

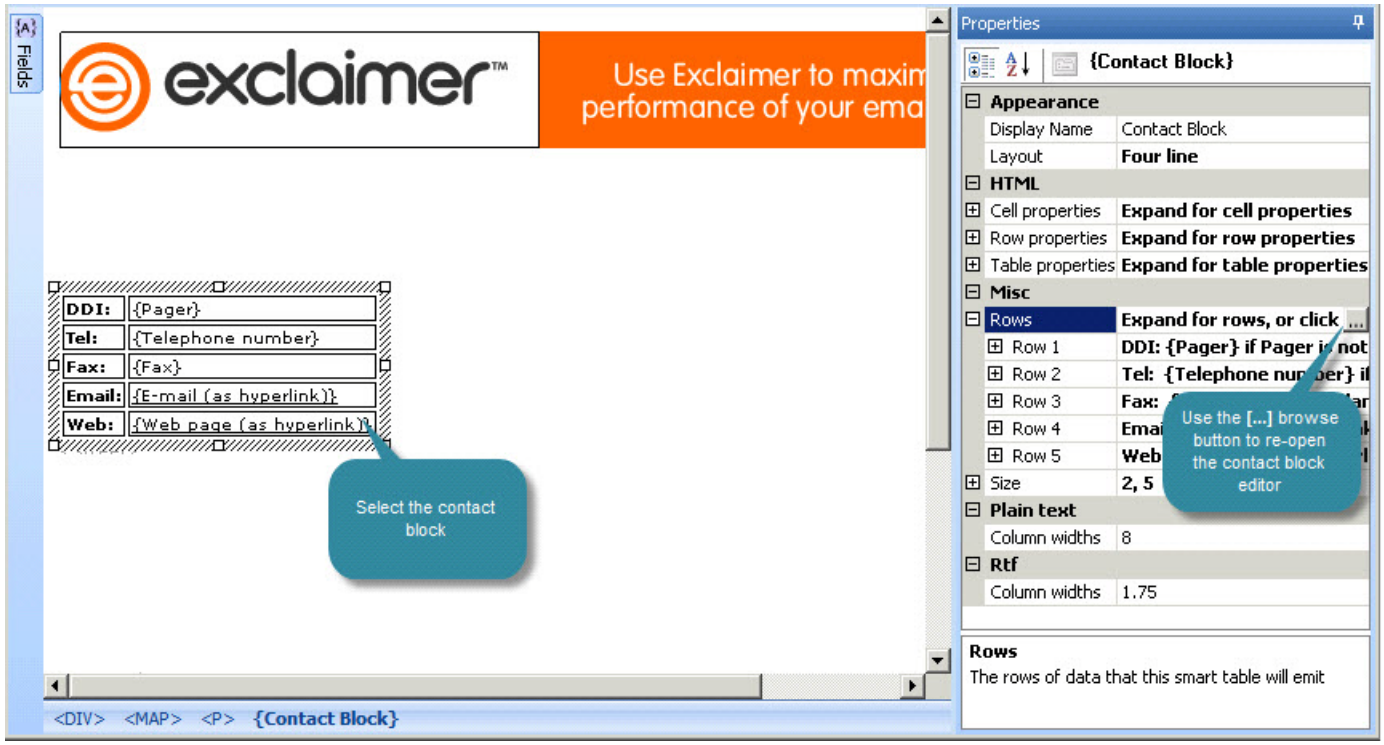


In this example, a department field has been added, but we have chosen to suppress this row if the sender's department field is blank. This means that the line will not be included if there is no information to show (thus avoiding blank lines).

Selecting the table option in the HTML editor [see page 195] displays an **insert table options** window, which includes the option to insert a contact block. If preferred, you can use this method to insert a contact block instead of adding the contact block field.

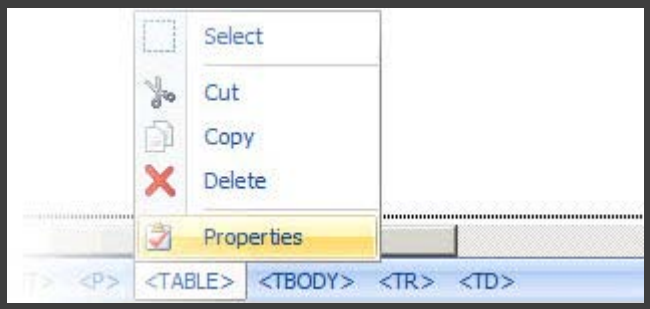
Updating an Existing Contact Block

To update an existing contact block in a template, simply select and double-click the required block. Alternatively, select the entire contact block and expand the misc section in the properties pane. From here, select the browse - ... - button to the right of the cell properties entry. The smart table rows window is displayed so you can add, edit or remove rows as required:



When working with any kind of table in the HTML template editor, it may be useful to note the 'HTML element trail' at the bottom of the editor window.:

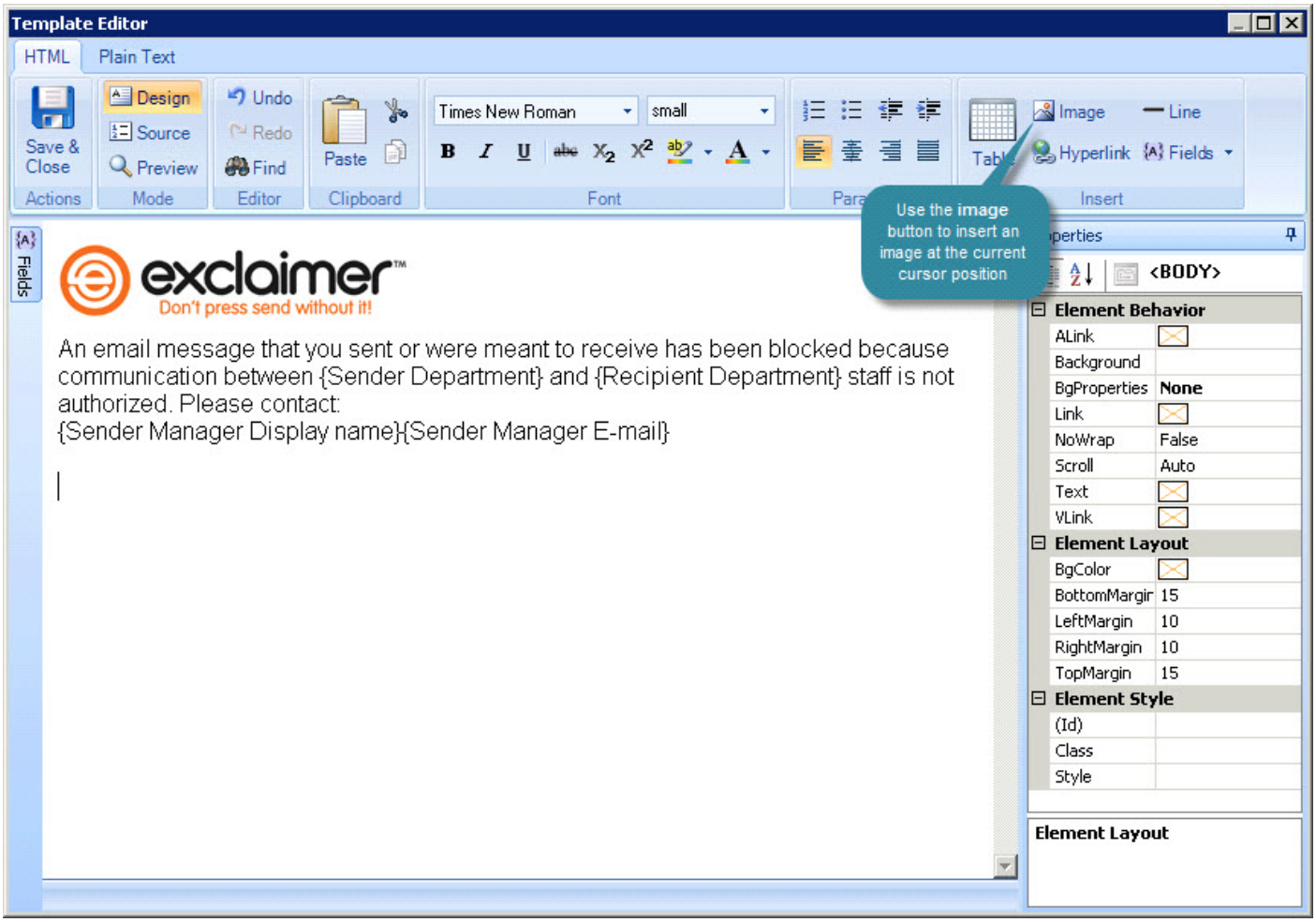
Depending on the size of your table, it can sometimes be tricky to select a particular row, column or cell, but you can do this very easily from the element trail - just click the required element. When you click on an element, further options are displayed:



Selecting properties will show properties for this table element in the properties pane [see page 225].

How do I Insert a Banner Image at the Start of Messages?

To insert a banner image at the very start of an automatic reply, position the cursor at the very start of the template editor and use the image button to insert the required image:



If you have a selection of banner images, you can take this a step further and use the rotating banner ad [see page 218] field to switch between all images in a given folder.

Other Resources

Exclaimer Support

World Wide Email Support: support@exclaimer.com
Exclaimer Knowledge Base: http://www.exclaimer.com/support-home/KB.aspx
Exclaimer Forums: http://www.exclaimer.com/cs/forums/default.aspx

UK - Telephone: +44 (0) 1252 531 422
USA & Canada - Telephone: +1-888-450-9631
South Africa - Telephone: +27 (0) 11 561 0900
Benelux - Telephone: +31 (0)228-567066
Germany - Telephone: +49 (0) 421 5371 458
Rest of the World, UK - Telephone: +44 (0) 1252 531 422

Exclaimer Sales

UK Sales: sales@exclaimer.com
Telephone: 01252 531422

US & Canada Sales: usasales@exclaimer.com
Telephone: +1-888-450-9631

Benelux Sales: sales@exclaimer.nl
Telephone: +31 (0)228-567066

Germany Sales: sales@exclaimer.de
Telephone: +31 (0)228-567066

South African Sales: sales@exclaimer.co.za
Telephone: +27 (0) 11 561 0900

Hungary Sales: sales@exclaimer.com
Telephone: +36 20 422 3984

France Sales: sales@exclaimer.com
Telephone: 00 33 4 76 21 17 03

Spain Sales: sales@exclaimer.es
Telephone: +34 947 257 714

Rest of the World (UK): sales@exclaimer.com
Telephone: +44 1252 531422

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 Auto Responder 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.

This document was last updated: 11th January 2011

Copyright 2011, 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.