Exclaimer Anti-spam
User Manual

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

Contents

Chapter 1

Getting Started

Exclaimer Anti-spam Overview

Microsoft Exchange incorporates sophisticated anti-spam technology but accessing and updating these features can be a daunting prospect even for the technically minded. At best, the user interface to some anti-spam features is less than intuitive and at worst, it is nonexistent and requires command line instructions.

Exclaimer Anti-spam has been designed to provide intuitive, user-friendly access to anti-spam settings within Microsoft Exchange, and to build upon these settings to provide an additional level of security in the fight against unsolicited commercial email (spam).

How Does It Work?

As part of the installation process for Exclaimer Anti-spam, any existing anti-spam settings are loaded from Microsoft Exchange.

Thereafter, if you change settings in Exclaimer Anti-spam, they will be applied to your Microsoft Exchange configuration. Conversely, any changes that might be made to anti-spam settings within Microsoft Exchange (directly) will be loaded into Exclaimer Anti-spam (either when the software is closed and restarted, or when you choose to refresh data [pg.54] whilst Exclaimer Anti-spam is running).

What Next?

Exclaimer Anti-spam works on a system of features [pg.120] and rules [pg.63]. In most cases, features and rules provide a layer over existing Microsoft Exchange settings. Features are used to define core configuration for Microsoft Exchange anti-spam filters and as such, these are always processed first. A series of rules are provided to access settings which are likely to be changed on a more regular basis; you can:

- Maintain a list of recipients for whom anti-spam tests will never be performed (using the recipient white list rule), see page 84.
- Maintain a list of senders who are considered to be 'safe' and for whom anti-spam tests will never be performed (using the sender white list rule), see page 77.
- Maintain a list of senders who are considered to be 'unsafe' and from whom email messages will be blocked (using the sender block list rule), see page 67.
- Specify actions to be taken with messages classified as spam as a result of content filtering (using the content filtering rule), see page 100.
- Specify actions to be taken with messages classified as spam as a result of checking the Sender ID (using the sender ID rule), see page 89.
- Specify actions to be taken with bulk email messages that are classified by Commtouch (using the Commtouch classifications rule), see page 106.

No Technical Expertise Required

Some organizations are fortunate to have experienced system administrators who have a detailed knowledge of Microsoft Exchange and its anti-spam settings - but many others do not. Exclaimer Anti-spam has been designed to suit the needs of both experienced and novice users.

When Exclaimer Anti-spam is installed, you are asked to choose an anti-spam scenario - in other words, to choose (at a high level) how you would like your anti-spam settings to work. A scenario is a set of predefined options for running Exclaimer Anti-spam in a particular way (for example, whether you wish to quarantine spam messages or reject them) and these options are applied once installation is complete.

If you have little or no experience with anti-spam settings, Exclaimer Anti-spam scenarios are the ideal way to get started. Having completed simple installation [pg.21] and setup [pg.24] wizards you can be sure that your Microsoft Exchange anti-spam filters are optimized and there is no need for you to change features [pg.120] or even rules [pg.63] unless you want to.

However, if you are a seasoned administrator, you will appreciate a clean, intuitive interface to access features [pg.120] and rules [pg.63] to customise a scenario.

But That's Not All...

For an extra level of security, Exclaimer Anti-spam is also fully integrated with the third party Commtouch [pg.106] anti-spam solution. Commtouch uses its own Recurrent Pattern Detection™ (RPD™) technology which focuses on detecting and classifying patterns in large scale spam attacks. These classifications are maintained in a vast database which can be interrogated by Exclaimer Anti-spam; this means that incoming email messages can be checked and classified in real time.

Closing Exclaimer Anti-spam

The Exclaimer Anti-spam application does not need to be running for rules [pg.63] and features [pg.120] to be processed. To close Exclaimer Anti-spam, select exit from the file menu at the top of the Exclaimer console [pg.32].

Chapter 2

Installation & Deployment

Installation Overview

Exclaimer Anti-spam can be installed on an Edge Transport Server or on a Hub Transport Server (see installation types [pg.14] for further information about these server types).

The installation process for Exclaimer Anti-spam is very straightforward, using an installation wizard to copy required files and complete most setup behind the scenes. Having completed the installation wizard [pg.21] for the first time, the setup wizard [pg.24] is launched automatically.

The setup wizard takes you through the basic setup required to get started with Exclaimer Anti-spam. Here, you are asked to choose the way in which you wish to run Exclaimer Anti-spam by choosing a scenario. A scenario is a set of predefined options for running Exclaimer Anti-spam in a particular way (for example, choose whether you wish to run in evaluation mode or in full deployed mode). Each scenario is optimized to eradicate spam.

Once Exclaimer Anti-spam is installed and you have had an opportunity to work with it for a while, you may decide that you wish to switch to a different scenario; you can change the active scenario at any time using Exclaimer Anti-spam options. [pg.58]

> The installation process is the same whether you are installing on an **Edge Transport Server** or on a **Hub Transport Server**.

In this chapter you will find information regarding all aspects of installation, including:

- Installation types; find out more about installing Exclaimer Anti-spam on Hub Transport servers and Edge Transport servers - see page 14 for details.
- System requirements; requirements are detailed for both installation types - see page 16 for details.
- Downloading Exclaimer Anti-spam; find out where you can download required installation files - see page 18 for details.
- System changes; find out what changes are made to your system when Exclaimer Anti-spam is installed - see page 19 for details.
- The installation and setup wizards; step through the installation and first-use setup processes - see pages 21 and 24 (respectively) for details.
- Command line installation; if you are installing Exclaimer Anti-spam at multiple locations, you may prefer to perform a ‘silent’ installation (i.e. bypass the installation wizard) - see page 29 for details.
- Uninstalling Exclaimer Anti-spam; find out about how to uninstall Exclaimer Anti-spam - see page 30 for details.

Installation Types

Exclaimer Anti-spam can be installed on an Edge Transport server or on a Hub Transport server.

Often, an Edge Transport server is a standalone Microsoft Exchange server which has the Edge Transport role installed. This server sits between the Internet and the rest of the Exchange Server organization - i.e. on the 'edge' of your network. Its purpose is to filter spam and malicious content before it reaches your network. Conversely, a Hub Transport server is a server (with the Hub Transport role installed) which sits within an Active Directory domain.

> In many cases, setup is such that the **Edge Transport server** is **not** a member of the Active Directory domain within an organization, however this does not have to be the case. If required, Microsoft does support **Edge Transport servers** that are members of the Active Directory domain.
>
> For example, smaller organizations are most likely to have one or two **Edge Transport servers**; given that these are effectively standalone machines it is fairly straightforward to configure each server individually. However, larger organizations are likely to have more **Edge Transport servers** which makes this impossible; in this situation, **Microsoft** recommend having **Edge Transport servers i**n their own **Active Directory** forest so they can be managed as a whole.

Edge Transport rules are used to protect Exchange organizations by applying rules to email messages and then taking appropriate action dependent upon whether messages pass or fail. Edge Transport rules are based upon SMTP addresses, MIME content, words in the subject or message body, and Spam Confidence Level ratings (SCL).

The Edge Transport server is also responsible for all mail entering the Exchange organization. Email messages travel inbound through the Edge Transport and, once Edge Transport rules have been applied, the messages are passed on to the Hub Transport server.

Considerations for Installing Exclaimer Anti-spam

The installation process is the same whether you are installing on an Edge Transport Server or on a Hub Transport Server.

If the software is installed on a Hub Transport Server that does not have Microsoft Exchange anti-spam agents installed, the Exclaimer Anti-spam installation process will install them with out-of-box Microsoft Exchange anti-spam configuration.

If the software is installed on a Hub Transport Server or an Edge Transport Server where Microsoft Exchange anti-spam agents are installed, the existing Microsoft Exchange anti-spam configuration is stored before the installation takes place. During the installation process, the Exclaimer Anti-spam SMTP Agent and the Exclaimer Anti-spam Routing Agent transport agents are installed into the Microsoft Exchange Transport Service.

In terms of processing sequence, these two agents are last in the list of Transport Agents (ordered SMTP and then Routing).

When the software is uninstalled the Microsoft Exchange anti-spam configuration is returned to the original configuration that was stored prior to installation.

System Requirements

System requirements for hardware and software are summarized in the following sections.

Requirements for the Exclaimer Console

Installing on a Hub Transport Server

Hardware

Item	Minimum Reqs	Recommended Reqs
CPU	x64 architecture-based computer	N/A
Memory	2GB	4GB
Disk Space	350MB	500MB
Screen Resolution	1024 x 768 pixels	1152 x 864 or higher

Note that Intel Itanium family IA64 processors are not supported.

Software

Item	Minimum Requirements
Operating Systems	Windows Server 2003 x64 (inc. all service pack levels) Windows Server 2003 R2 x64 (inc. all service pack levels) Windows Server 2008 x64 (inc. all service pack levels) Windows Server 2008 R2 Windows Small Business Server 2008 Windows Small Business Server 2011
Exchange Server Roles	Microsoft Exchange Server 2007 SP1 or above - Hub Transport Role Microsoft Exchange Server 2010 - Hub Transport Role
Microsoft .NET Framework	Microsoft .Net Framework 3.5

Installing on an Edge Transport Server

Hardware

Item	Minimum Reqs	Recommended Reqs
CPU	x64 architecture-based computer	N/A
Memory	2GB	4GB
Disk Space	350MB	500MB
Screen Resolution	1024 x 768 pixels	1152 x 864 or higher

Note that Intel Itanium family IA64 processors are not supported.

Software

Item	Minimum Requirements
Operating Systems	Windows Server 2003 x64 (all versions) Windows Server 2003 R2 x64 Windows Server 2008 x64 Windows Server 2008 R2
Active Directory Forest	Active Directory must be at Windows Server 2003 forest functionality level (or higher) -or- Active Directory Application Mode (ADAM) -or- Active Directory Lightweight Directory Services (ADLDS)
Exchange Server Roles	Microsoft Exchange Server 2007 SP1 or above – Edge Transport Role Microsoft Exchange Server 2010 – Edge Transport Role
Microsoft .NET Framework	Microsoft .Net Framework 3.5

Downloading Anti-spam

The Exclaimer Anti-spam installation file is named setup.exe and can be downloaded from the Exclaimer products page (http://www.exclaimer.com/products/Overview.aspx).

The same installation file is used irrespective of whether you are installing Exclaimer Anti-spam on a Hub Transport server or on an Edge Transport server.

Once downloaded, setup.exe should be run on the required Microsoft Exchange Server.

If required, an **MSI** is available from support by contacting support@exclaimer.com.

System Changes

The installation process makes the following changes to your system:

- If you install the software on a Hub Transport Server where Microsoft Exchange Anti spam agents **are not** installed, the Exclaimer Anti-spam installation wizard will install them (having stored a copy of the out-of-box Microsoft Exchange Anti spam configuration first).

- If you install Exclaimer Anti-spam on a Hub Transport Server where Microsoft Exchange Anti spam agents **are** installed, or if you install on an Edge Transport Server, the existing Microsoft Exchange Anti spam configuration is stored before installation takes place.

- During the Exclaimer Anti-spam installation, the following agents are installed:

    - The Exclaimer Anti-spam SMTP Agent
    - The Exclaimer Anti-spam Routing Agent

    Transport Agents are installed into the Microsoft Exchange Transport Service. In the processing order, these two agents are last in the list of Transport Agents (ordered SMTP then Routing).

File Location(s)

As part of the installation process, you are asked to specify a destination folder, into which program files will be installed. The default folder is C:\Program Files\Exclaimer Ltd\Anti-spam.

In addition to program files, a number of configuration files are copied to your system. The location of these files varies according to operating system, as summarized below:

Operating System	Location
Windows Server 2003 x64 Windows Server 2003 R2 x64	\Documents and Settings\All Users\Application Data\Exclaimer Ltd\Anti-spam
Windows Server 2008 x64 Windows Server 2008 R2 x64 Windows Small Business Server 2008 Windows Small Business Server 2011	\ProgramData\Exclaimer Ltd\Anti-spam

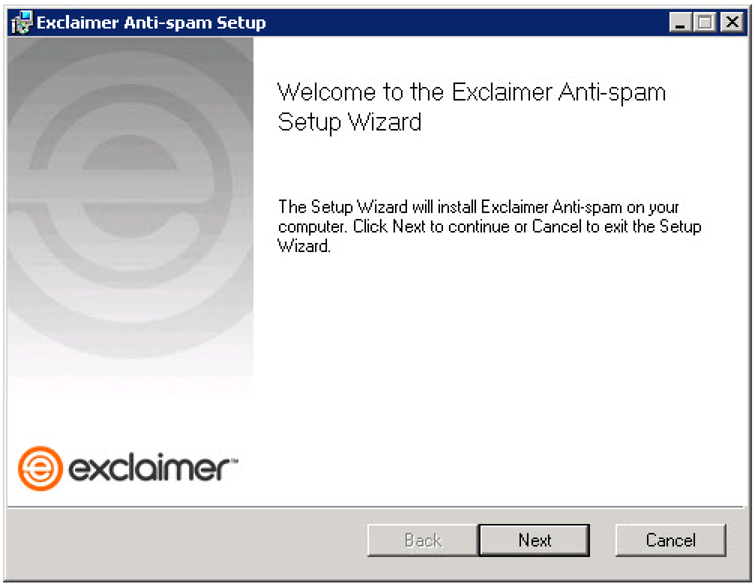
The Installation Wizard

The installation process for Exclaimer Anti-spam is completed using a familiar 'wizard' approach to guide you through each process, step-by-step.

This process includes the Exclaimer license agreement and copies files to your preferred destination folder. Once complete, you can use the application for five days, after which you must register for a 30 day trial [pg.42] to continue using Anti-spam.

To complete the installation wizard, follow the steps below:

1. Double click the setup file to start the installation and display a welcome message:

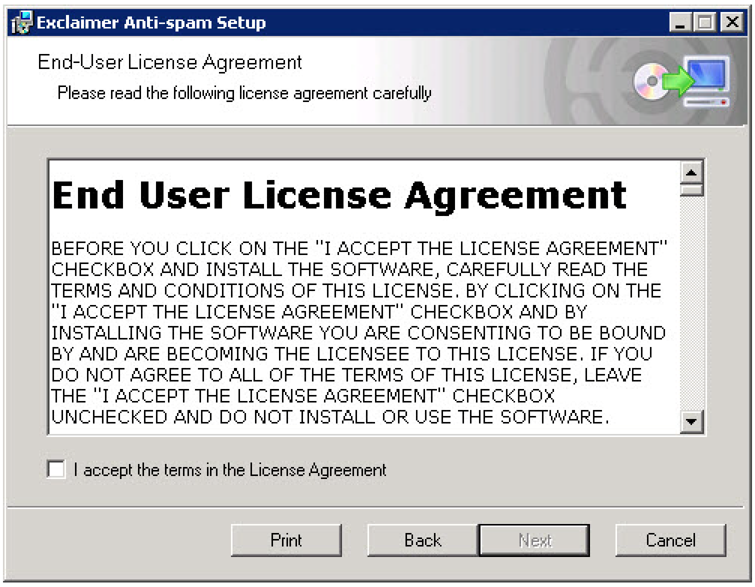


Exclaimer Anti-spam Setup

Welcome to the Exclaimer Anti-spam Setup Wizard

The Setup Wizard will install Exclaimer Anti-spam on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Click the next button to view the end-user license agreement:



Exclaimer Anti-spam Setup

End-User License Agreement

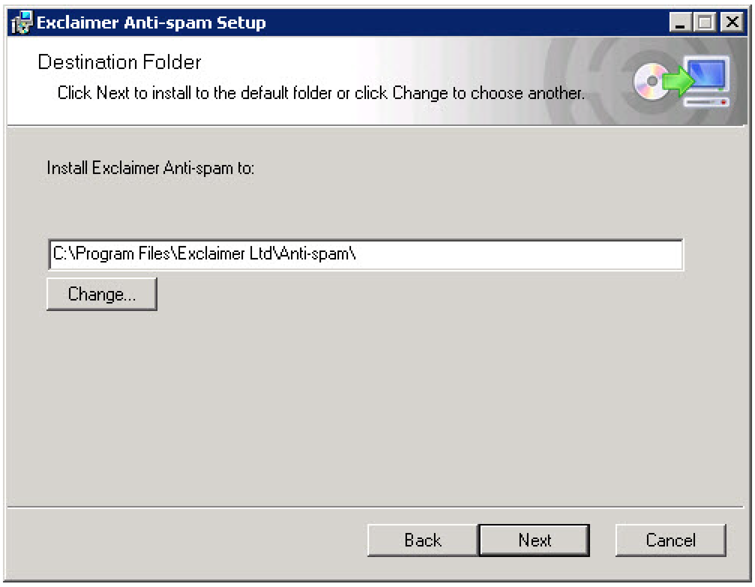
Please read the following license agreement carefully

End User License Agreement

BEFORE YOU CLICK ON THE "I ACCEPT THE LICENSE AGREEMENT" CHECKBOX AND INSTALL THE SOFTWARE, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS LICENSE. BY CLICKING ON THE "I ACCEPT THE LICENSE AGREEMENT" CHECKBOX AND BY INSTALLING THE SOFTWARE YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING THE LICENSEE TO THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, LEAVE THE "I ACCEPT THE LICENSE AGREEMENT" CHECKBOX UNCHECKED AND DO NOT INSTALL OR USE THE SOFTWARE.

☐ I accept the terms in the License Agreement

3. Having read the license agreement, check the I accept the terms in the license agreement box and click next to specify a destination folder for installed files:



Exclaimer Anti-spam Setup

Destination Folder

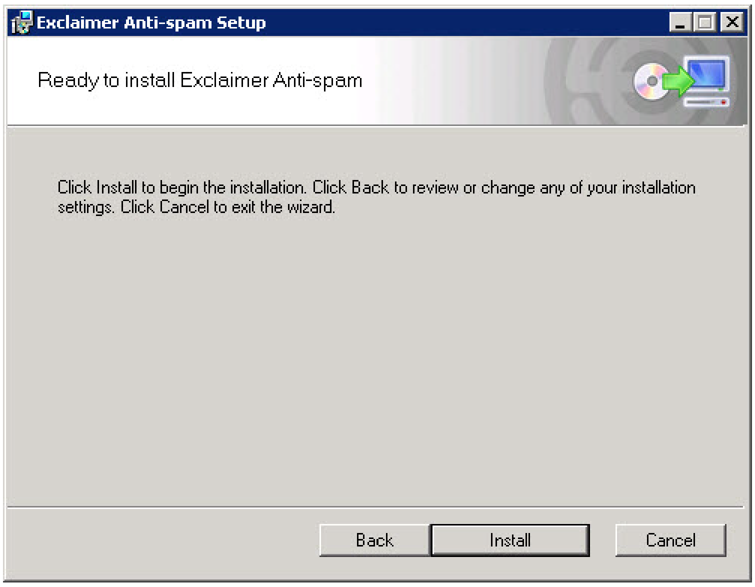
Click Next to install to the default folder or click Change to choose another.

Install Exclaimer Anti-spam to:

C:\Program Files\Exclaimer Ltd\Anti-spam\

From here you can accept the default folder, or click to specify a new location.

4. Click next to review:

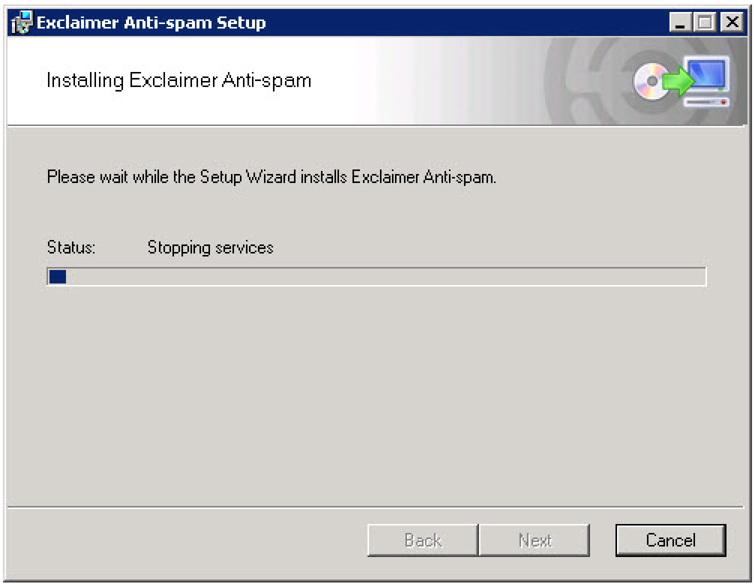


Exclaimer Anti-spam Setup

Ready to install Exclaimer Anti-spam

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click the install button to perform the installation:



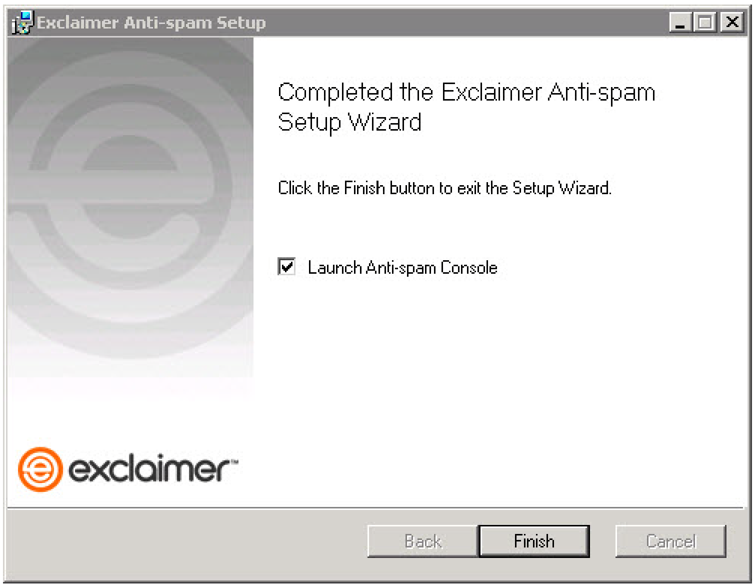
Exclaimer Anti-spam Setup

Installing Exclaimer Anti-spam

Please wait while the Setup Wizard installs Exclaimer Anti-spam.

Status: Stopping services

6. Progress is displayed on screen and final confirmation is shown upon completion:



Exclaimer Anti-spam Setup

Completed the Exclaimer Anti-spam Setup Wizard

Click the Finish button to exit the Setup Wizard.

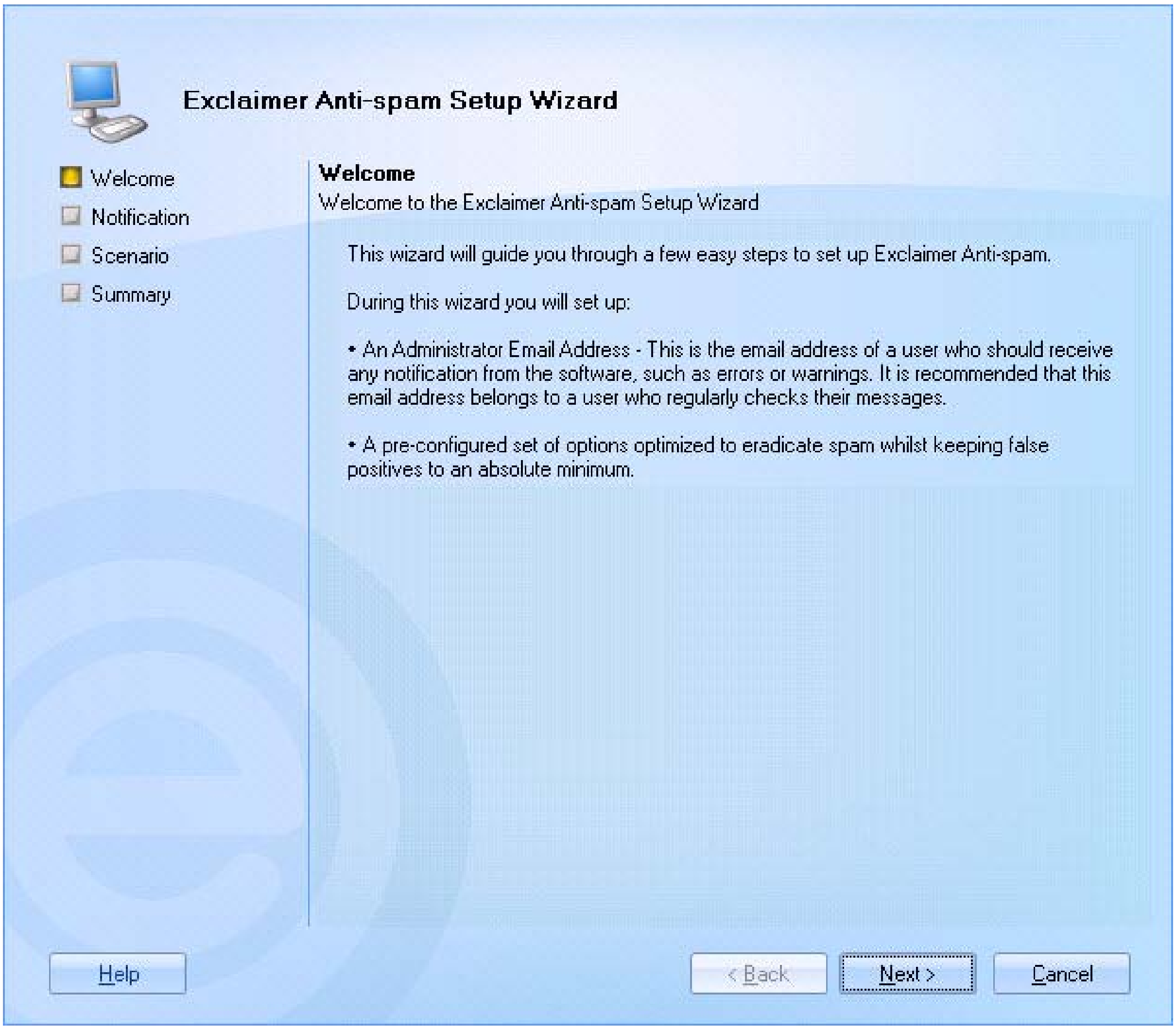
☑ Launch Anti-spam Console

7. Click finish to close the wizard. If you are installing Anti-spam for the first time, the setup wizard [pg.24] is launched. You should complete this wizard to choose how you wish to use Exclaimer Anti-spam and set basic settings to get started.

The Setup Wizard

Having completed the installation wizard [pg.21] for the first time, the setup wizard is launched automatically. This wizard takes you through the basic setup required to get started with Exclaimer Anti-spam. To complete this wizard, follow the steps below:

1. The first stage of the setup wizard displays summary information about the process:



Exclaimer Anti-spam Setup Wizard

Welcome

Welcome to the Exclaimer Anti-spam Setup Wizard

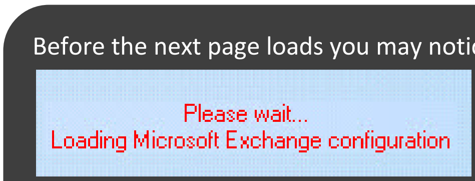
This wizard will guide you through a few easy steps to set up Exclaimer Anti-spam.

During this wizard you will set up:

• An Administrator Email Address - This is the email address of a user who should receive any notification from the software, such as errors or warnings. It is recommended that this email address belongs to a user who regularly checks their messages.

• A pre-configured set of options optimized to eradicate spam whilst keeping false positives to an absolute minimum.

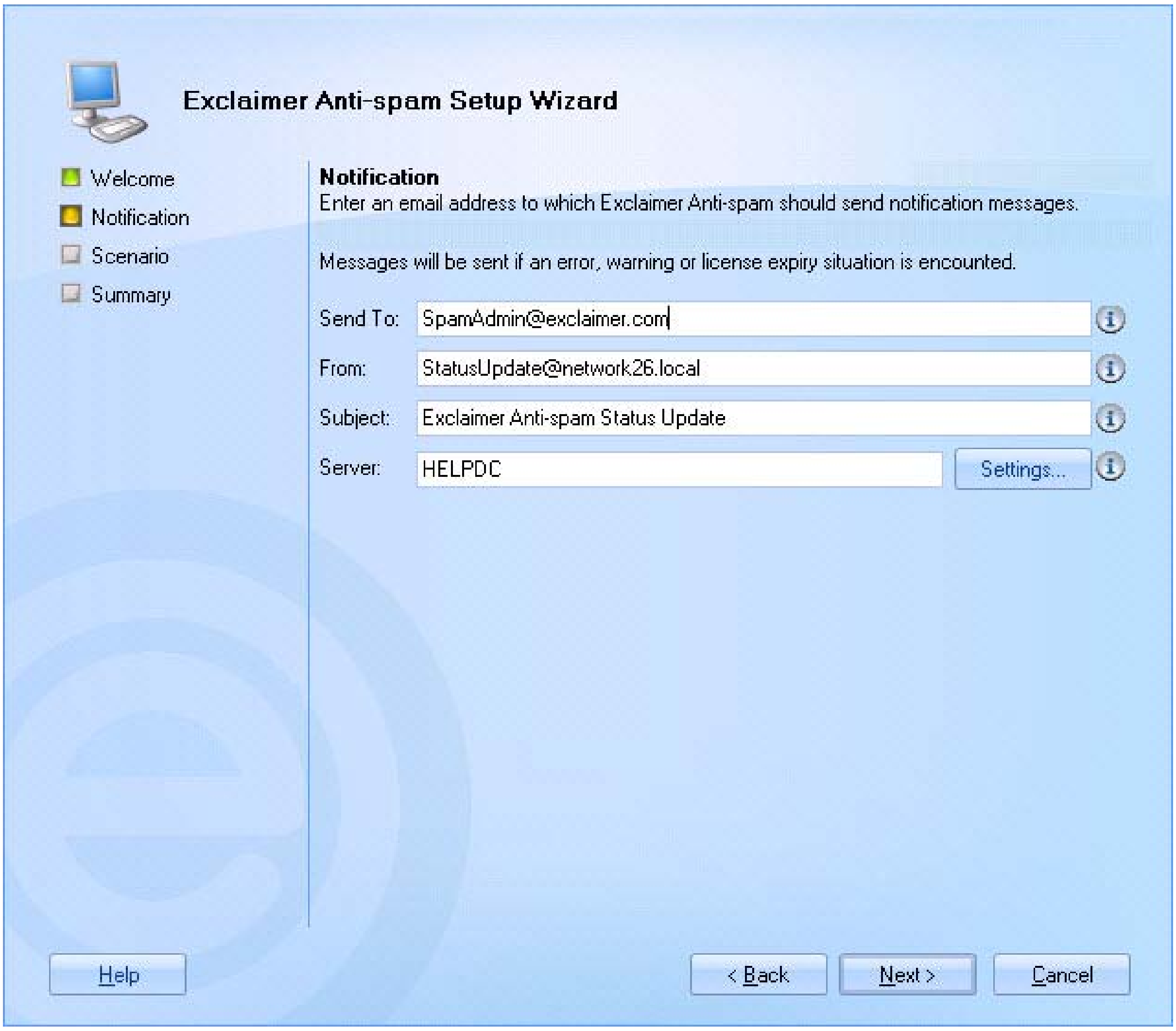
Before the next page loads you may notice a message similar to that shown below:



Please wait...
Loading Microsoft Exchange configuration

As part of the installation process, Exclaimer Anti-spam checks for and loads existing Microsoft Exchange anti-spam settings.

2. Click next to move to the next stage and define how email notifications are sent and received. Here, you can set an administrator email address to receive Exclaimer Anti-spam notifications, together with a sending address, subject line and server settings for notification messages:



Exclaimer Anti-spam Setup Wizard

Notification

Enter an email address to which Exclaimer Anti-spam should send notification messages.

Messages will be sent if an error, warning or license expiry situation is encounted.

Send To: SpamAdmin@exclaimer.com

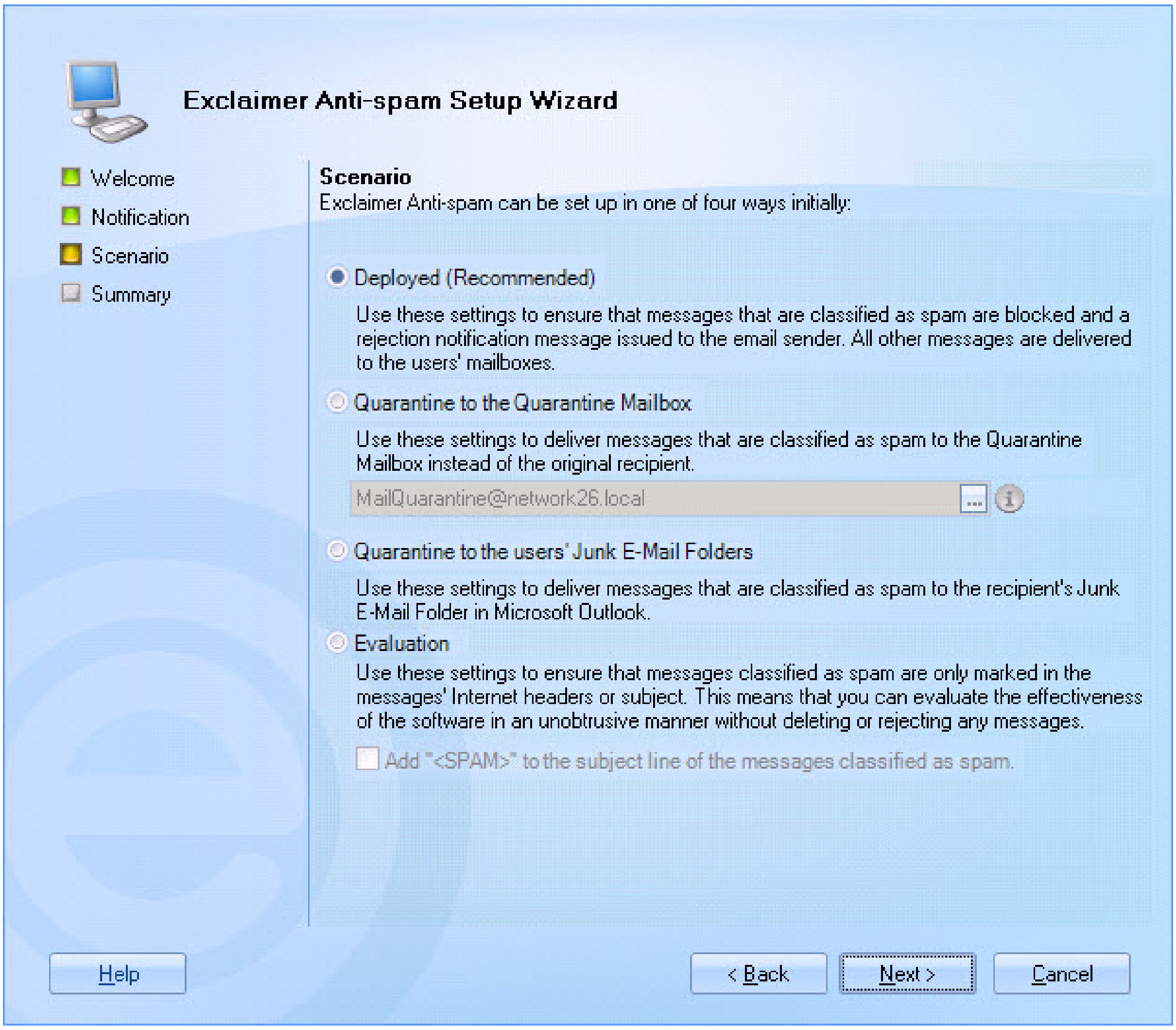
From: StatusUpdate@network26.local

Subject: Exclaimer Anti-spam Status Update

Server: HELPDC

For further information about these settings please see Exclaimer console settings on page 39.

3. Enter required details and click next to move to the next stage and choose a deployment scenario:



Scenario

Exclaimer Anti-spam can be set up in one of four ways initially:

● Deployed (Recommended)

Use these settings to ensure that messages that are classified as spam are blocked and a rejection notification message issued to the email sender. All other messages are delivered to the users' mailboxes.

○ Quarantine to the Quarantine Mailbox

Use these settings to deliver messages that are classified as spam to the Quarantine Mailbox instead of the original recipient.

MailQuarantine@network26.local

○ Quarantine to the users' Junk E-Mail Folders

Use these settings to deliver messages that are classified as spam to the recipient's Junk E-Mail Folder in Microsoft Outlook.

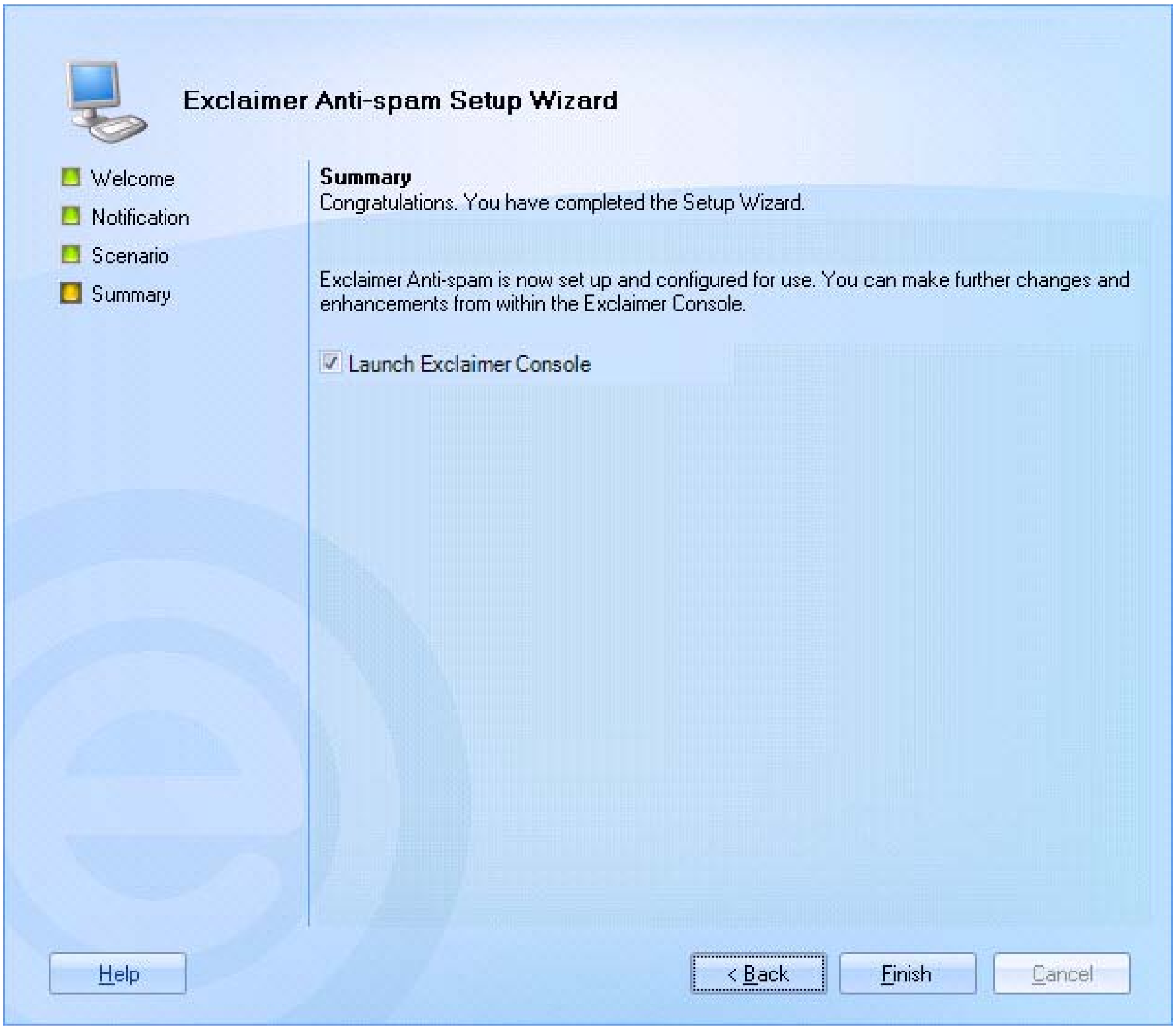
○ Evaluation

Use these settings to ensure that messages classified as spam are only marked in the messages' Internet headers or subject. This means that you can evaluate the effectiveness of the software in an unobtrusive manner without deleting or rejecting any messages.

□ Add "<SPAM>" to the subject line of the messages classified as spam.

A **scenario** is a set of predefined options for running **Exclaimer Anti-spam** in a particular way. Each **scenario** is optimized to eradicate spam. Once **Exclaimer Anti-spam** is installed you can change the active scenario at any time using Exclaimer Anti-spam options [pg.58].

4. Ensure that the required scenario is selected and click next to move to the next page. If a direct connection to the Internet is detected, the final summary page is displayed:



Exclaimer Anti-spam Setup Wizard

Summary

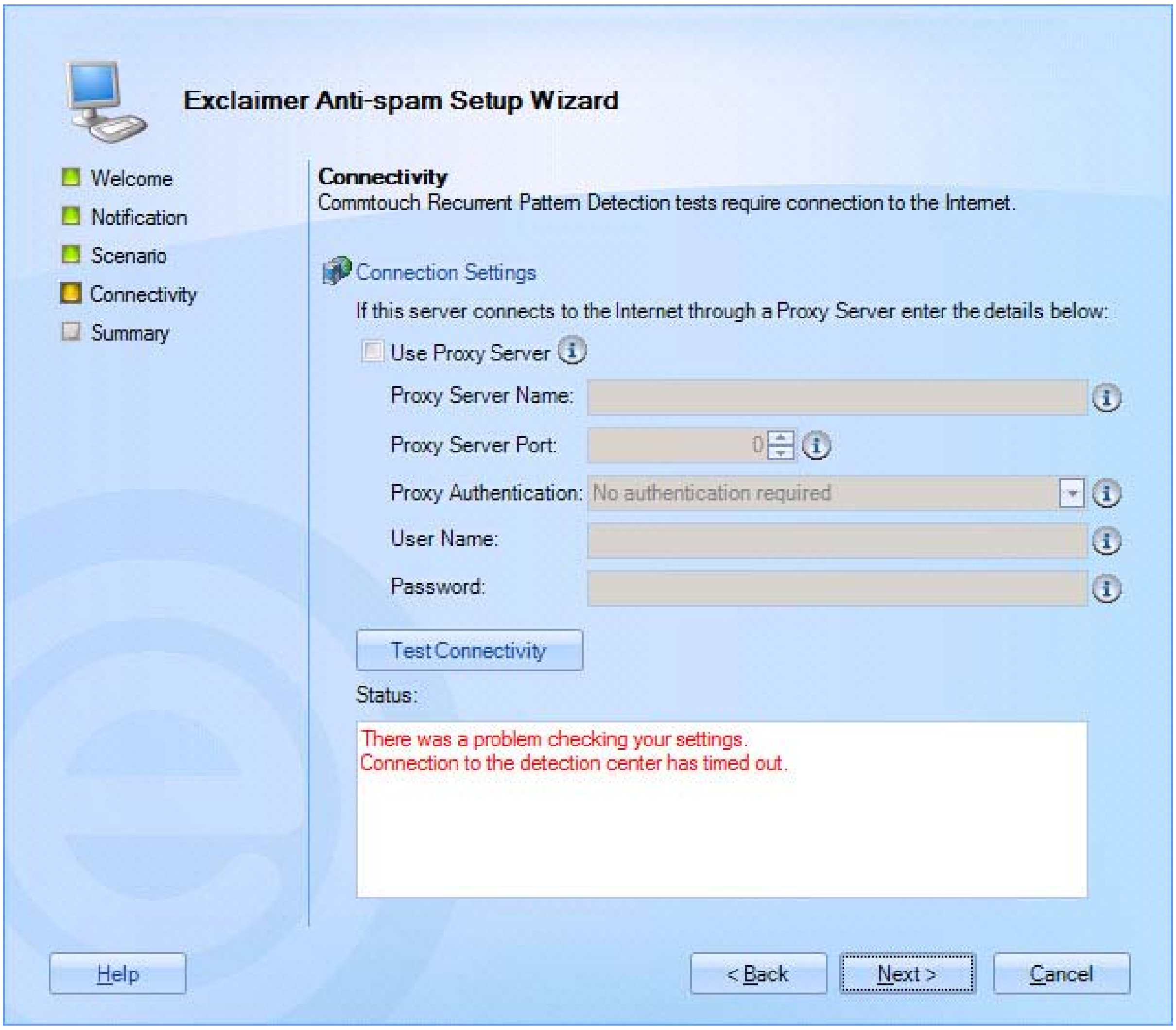
Congratulations. You have completed the Setup Wizard.

Exclaimer Anti-spam is now set up and configured for use. You can make further changes and enhancements from within the Exclaimer Console.

☑ Launch Exclaimer Console

5. Click finish to exit and launch Exclaimer Anti-spam.

6. If a direct Internet connection is not detected, an additional connectivity page is displayed:



Exclaimer Anti-spam Setup Wizard

🟩 Welcome
🟩 Notification
🟩 Scenario
🟧 Connectivity
□ Summary

Connectivity
Commtouch Recurrent Pattern Detection tests require connection to the Internet.

Connection Settings

If this server connects to the Internet through a Proxy Server enter the details below:

□ Use Proxy Server

Proxy Server Name:

Proxy Server Port: 0

Proxy Authentication: No authentication required

User Name:

Password:

Test Connectivity

Status:

There was a problem checking your settings.
Connection to the detection center has timed out.

An Internet connection is required for the integrated Commtouch solution [pg.106]. If you need to access the Internet through a proxy server, settings must be defined here (for further information about these settings please refer to the connectivity section of this guide on page 193).

7. Having defined required connection settings, use the test connectivity button to test these settings and ensure that a connection to the Commtouch database can be made.

Exclaimer Anti-spam requires an Internet connection. If a direct Internet connection is not detected, you must define connectivity settings and use **the test connectivity** button to confirm these settings before you will be able to proceed.

Command Line Installation

To save time, you can perform a 'silent' installation using command line options. A command line installation installs Exclaimer Anti-spam without the need to go through the installation wizard [pg.21].

Programs and services are installed and when Exclaimer Anti-spam is opened, the setup wizard [pg.24] is launched.

Required Preparation

Command line installations are run using an MSI installation file, rather than the standard setup.exe. To obtain the required MSI installation file, please contact Exclaimer support (support@exclaimer.com).

Supported Command Line Options

The following options are supported for a command line installation:

Parameter	Description
INSTALLLOCATION	Where the application should be installed. This corresponds to the Installation Directory screen in the standard installation wizard.

For example:

```
“Anti-spam Install.msi" /qn INSTALLLOCATION="D:\Program Files\Exclaimer Ltd\Anti-spam\"
```

Note that environment variables cannot be used in paths - you must specify full paths explicitly.

Uninstalling Anti-spam

When Exclaimer Anti-spam is installed, your existing Microsoft Exchange Anti spam configuration is backed up and stored. When Exclaimer Anti-spam is uninstalled the Microsoft Exchange Anti spam configuration is returned to its original state.

The uninstall process removes the following items for Exclaimer Anti-spam:

- Application program files
- The Exclaimer Anti-spam SMTP Agent
- The Exclaimer Anti-spam Routing Agent

Your Exclaimer Anti-spam configuration files are not removed as part of the uninstall process. The location of these files on your system depends upon which operating system is in use, as summarized below:

Operating System	Location
Windows Server 2003 x64 Windows Server 2003 R2 x64	\Documents and Settings\All Users\Application Data\Exclaimer Ltd\Anti-spam
Windows Server 2008 x64 Windows Server 2008 R2 x64 Windows Small Business Server 2008 Windows Small Business Server 2011	\ProgramData\Exclaimer Ltd\Anti-spam

Preparation

As a precaution you may wish to export your configuration before running the uninstall process.

The export includes all settings for Exclaimer Anti-spam. These are written to an econfig file, a proprietary file type for Exclaimer products. To export current settings, follow the steps below:

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

Running the Uninstall Process

There are two ways to start the uninstall process for Anti-spam:

- Activate the original setup.exe or the MSI file and choose the uninstall option; then follow on-screen instructions
- Use Add/Remove Programs in Windows Server 2003 or Programs and Features in Windows Server 2008; then follow on-screen instructions.

Chapter 3

The Exclaimer Console

Introduction

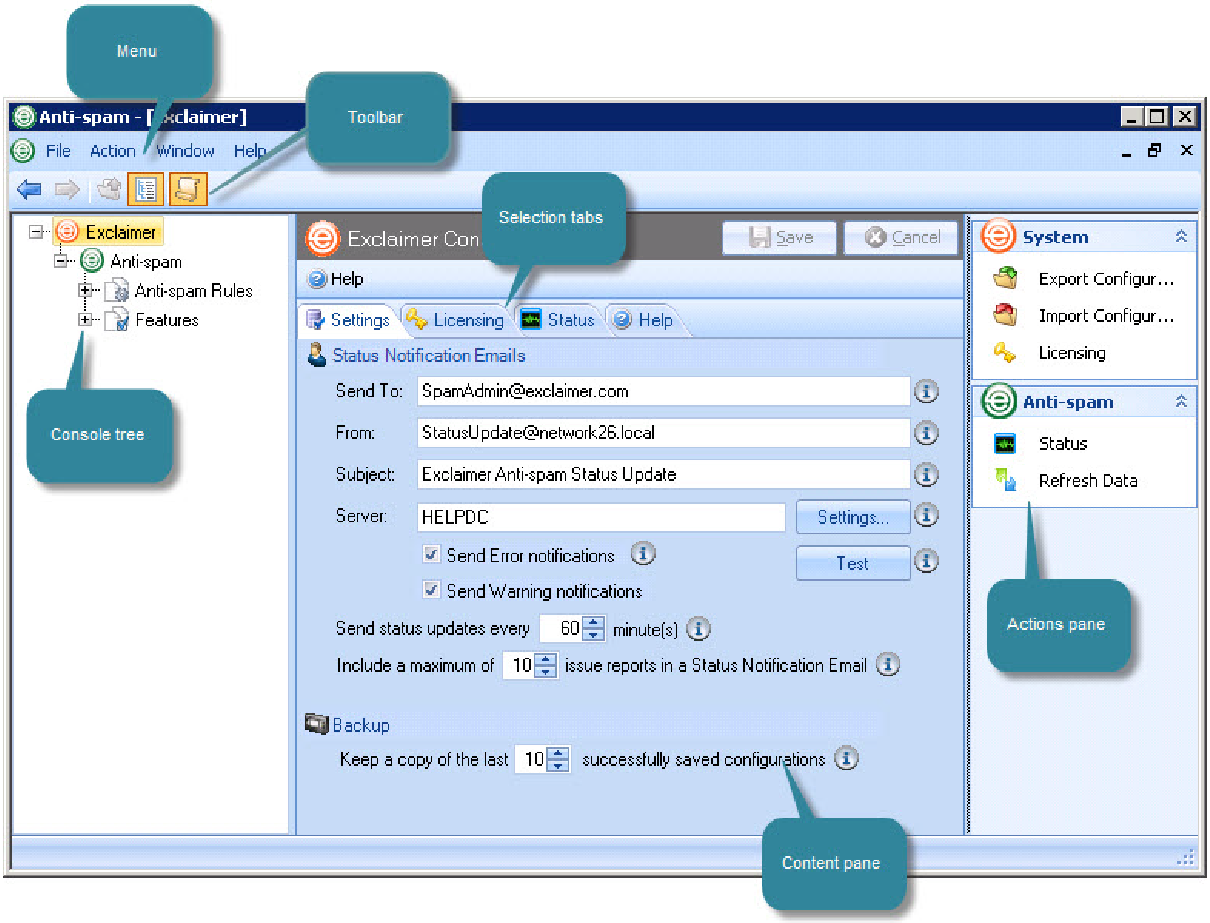
The Exclaimer console can be thought of as the 'control centre' for Exclaimer Anti-spam. From here, you can define general settings which are applicable to the system as a whole, and access each section of the application. This section explains how the Exclaimer console is used, including:

- Understanding the Exclaimer Console window [pg.34]
- Exclaimer console settings [pg.39]
- Exclaimer console licensing [pg.42]
- Exclaimer console status [pg.45]
- Exporting configuration settings [pg.51]
- Importing configuration settings [pg.52]
- Refreshing data from Microsoft Exchange [pg.54]

If you already know about the console and wish to get started with Exclaimer Anti-spam, see the Anti Spam [pg.56] section of this guide.

Understanding the Exclaimer Console Window

The Exclaimer console window is split into three panes, as shown below:



Status Notification Emails

Send To: SpamAdmin@exclaimer.com

From: StatusUpdate@network26.local

Subject: Exclaimer Anti-spam Status Update

Server: HELPDC Settings...

☑ Send Error notifications Test

☑ Send Warning notifications

Send status updates every 60 minute(s)

Include a maximum of 10 issue reports in a Status Notification Email

Backup

Keep a copy of the last 10 successfully saved configurations

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

- Console menu [pg.34]
- Console toolbar [pg.54]
- Console tree [pg.37]
- Content pane [pg.38]
- Selection tabs [pg.38]
- Actions pane [pg.38]

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 current content pane [pg.38]. **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 [pg.37] is currently selected. Those listed below are available when the top level (Exclaimer) branch is selected: **Export Configuration...** Use this option to export current configuration settings [pg.51] for the console. **Import Configuration...** Use this option to import current configuration settings [pg.52] for the console.
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 [pg.35], but have been placed on the toolbar for faster access. Options on this toolbar vary, depending on which branch of the console tree [pg.37] is currently selected.

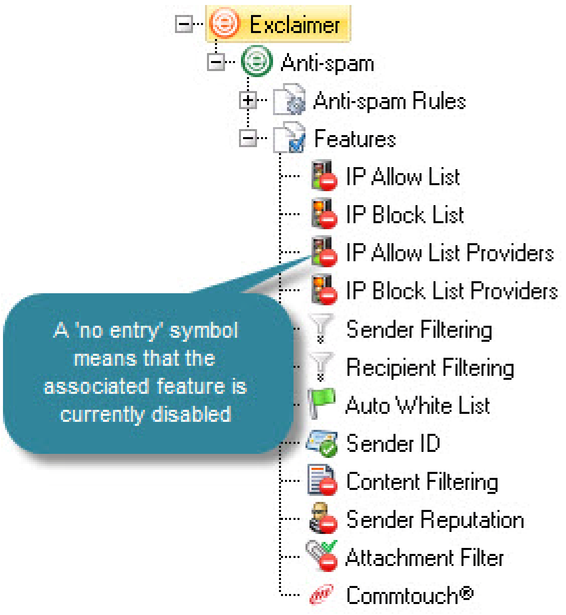
Those listed below are available when the top level (Exclaimer) branch is selected:

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 [pg.36] can be used to quickly navigate between branches within the console tree.

If a branch is associated with a 'no entry' symbol, it means that the feature is currently disabled:



A 'no entry' symbol means that the associated feature is currently disabled

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 [pg.38] 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 here are available when the top level (Exclaimer) branch is selected (settings [pg.39], licensing [pg.42] and status [pg.45]).

The Actions Pane

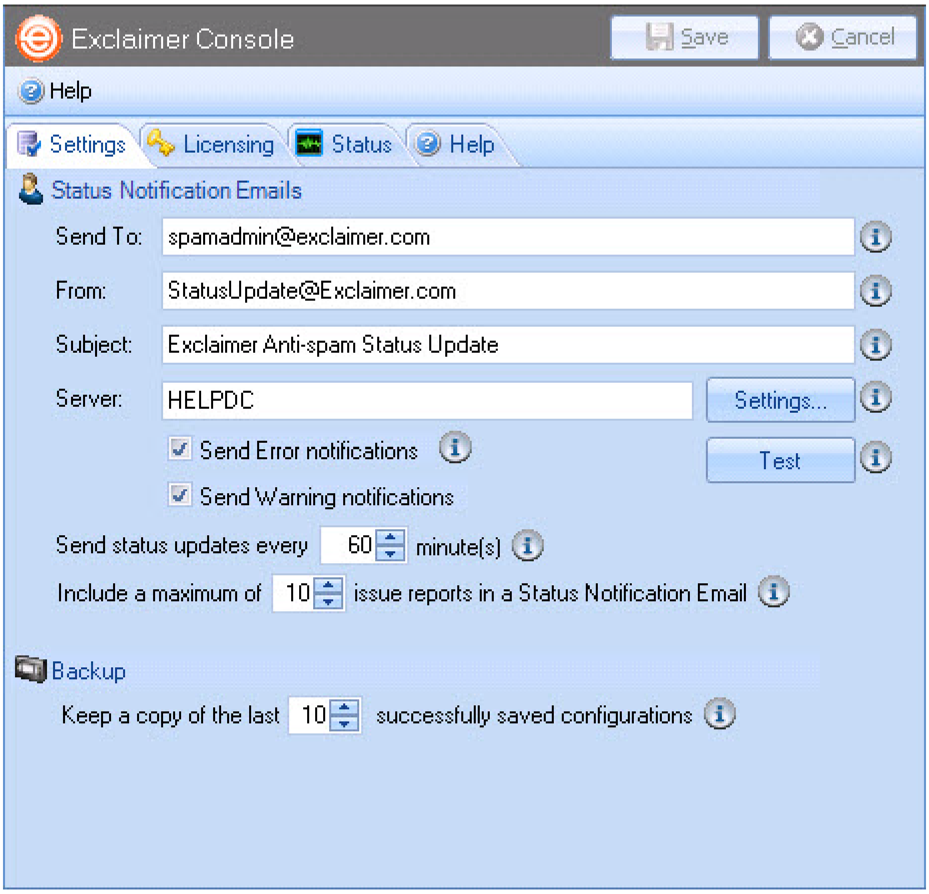
The actions pane displays quick access to common tasks, as summarized below:

Action	Select this option to...
System	
Export configuration...	Export all settings - see the export configuration... [pg.51] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [pg.52] page.
Licensing	Access the licensing tab to view licensing information [pg.42].
Anti Spam	
Status	View status information [pg.45] for Exclaimer Anti-spam.
Refresh data	Refresh the current configuration with anti-spam settings from Exchange. Note that any unsaved changes will be lost if you perform a refresh.

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 for defining how email notifications are sent and received, together with backup details:



Status Notification Emails

Send To: spamadmin@exclaimer.com

From: StatusUpdate@Exclaimer.com

Subject: Exclaimer Anti-spam Status Update

Server: HELPDC

☑ Send Error notifications

☑ Send Warning notifications

Send status updates every 60 minute(s)

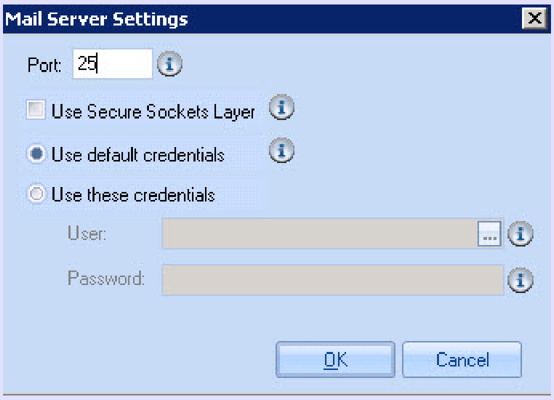
Include a maximum of 10 issue reports in a Status Notification Email

Backup

Keep a copy of the last 10 successfully saved configurations

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 (see page 49) across all tabs. Alternatively, use the **cancel** button to abandon all changes.

Fields on this tab are summarized below:

<table>
<tr><th>Option</th><th>Summary</th></tr>
<tr><td colspan="2"><b>Status Notification Emails</b></td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Send to</td><td>Specify an email account to receive notification emails.</td></tr>
<tr><td>From</td><td>Specify an email account to be displayed as the sender of notification emails.</td></tr>
<tr><td>Subject</td><td>Specify a subject line for notification emails.</td></tr>
<tr><td>Server</td><td>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:


Mail Server Settings
Port: 25
☐ Use Secure Sockets Layer
● Use default credentials
○ Use these credentials
User:
Password:
<table>
<tr><td>Port</td><td>Select the port number on which your mail server listens for email send requests. Typically, this is set to 25.</td></tr>
<tr><td>Use Secure Sockets Layer</td><td>Choose whether your mail server requires an SSL connection for email send requests. Typically, this is set to off.</td></tr>
<tr><td>Use default credentials / Use these credentials</td><td>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.</td></tr>
<tr><td>User</td><td>Your mail server will use credentials of the specified user when sending emails.</td></tr>
<tr><td>Password</td><td>Specify the appropriate password for the user specified for sending emails.</td></tr>
</table>
</td></tr>
</table>

.../continued

Option	Summary
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.
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 [pg.45] 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.

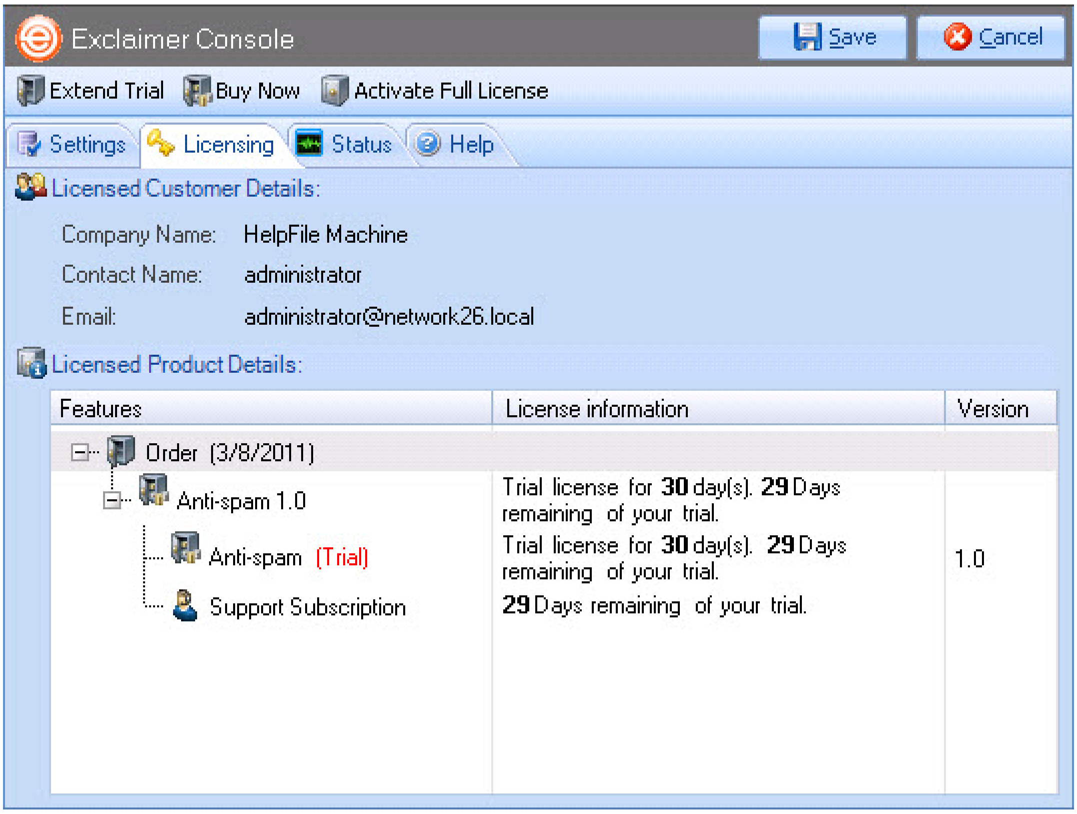
Actions

The following actions are available from the settings tab:

Action	Select this option to...
System	
Export configuration...	Export all settings - see the export configuration... [pg.51] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [pg.52] page.
Licensing	Access the licensing tab to view licensing information [pg.42].
Anti Spam	
Status	View status information [pg.45] for Exclaimer Anti-spam.
Refresh data	Refresh the current configuration with anti-spam settings from Exchange. Note that any unsaved changes will be lost if you perform a refresh.

Exclaimer Console Licensing

The licensing tab contains information and regarding licenses for Exclaimer Anti-spam:



Licensed Customer Details:

Company Name: HelpFile Machine

Contact Name: administrator

Email: administrator@network26.local

Licensed Product Details:

Features	License information	Version
Order (3/8/2011)		
Anti-spam 1.0	Trial license for **30** day(s). **29** Days remaining of your trial.	
Anti-spam (Trial)	Trial license for **30** day(s). **29** Days remaining of your trial.	1.0
Support Subscription	**29** Days remaining of your trial.	

Licensing information is summarized in the following sections:

- The licensing process [pg.43]
- Licensing information [pg.43]
- The licensing toolbar [pg.43]
- Actions [pg.44]

The Licensing Process

Our aim is to get you working with Exclaimer software as quickly as possible. As such, we have implemented a flexible licensing policy with minimal restrictions during the trial period.

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 a trial period, you can:

- Purchase and then activate the license.
- Contact the Exclaimer sales team to extend your trial (sales@exclaimer.com).

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).

The Licensing Toolbar

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

Toolbar Option	Summary
Register for 30 day trial	This option can be used if your initial five days usage is complete and you wish to have a longer evaluation period.
Extend trial	This option is only displayed if you have registered for a 30 day trial.
Buy now	Access the Exclaimer website products page (http://www.exclaimer.com/products.aspx) to purchase a license.
Activate full license	Having purchased a license, you will receive an email which includes a product activation key.

Actions

The following actions are available from the licensing tab:

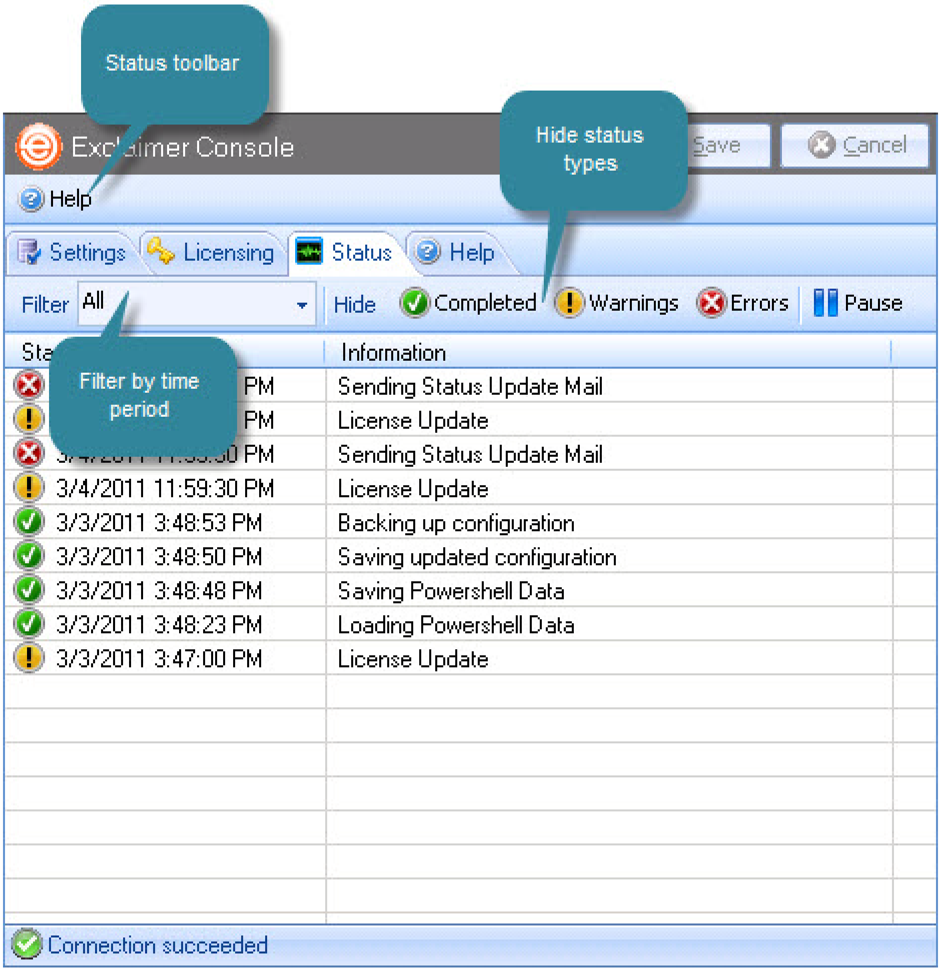
Action	Select this option to...
System	
Export configuration...	Export all settings - see the export configuration... [pg.51] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [pg.52] page.
Licensing	Access the licensing tab to view licensing information [pg.42].
Anti Spam	
Status	View status information [pg.45] for Exclaimer Anti-spam.
Refresh data	Refresh the current configuration with anti-spam settings from Exchange. Note that any unsaved changes will be lost if you perform a refresh.

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 (see page 49) across all tabs. Alternatively, use the **cancel** button to abandon all changes.

Exclaimer Console Status

The status tab contains information and actions regarding activity within the Exclaimer console - you can double click an entry in the list to view further details.

Entries are categorised as completed, warnings or errors, as shown:



Status toolbar

Hide status types

Filter by time period

Sta		Information
✗	PM	Sending Status Update Mail
!	PM	License Update
✗	[illegible] PM	Sending Status Update Mail
!	3/4/2011 11:59:30 PM	License Update
✓	3/3/2011 3:48:53 PM	Backing up configuration
✓	3/3/2011 3:48:50 PM	Saving updated configuration
✓	3/3/2011 3:48:48 PM	Saving Powershell Data
✓	3/3/2011 3:48:23 PM	Loading Powershell Data
!	3/3/2011 3:47:00 PM	License Update

Connection succeeded

Available options are summarized in the following sections:

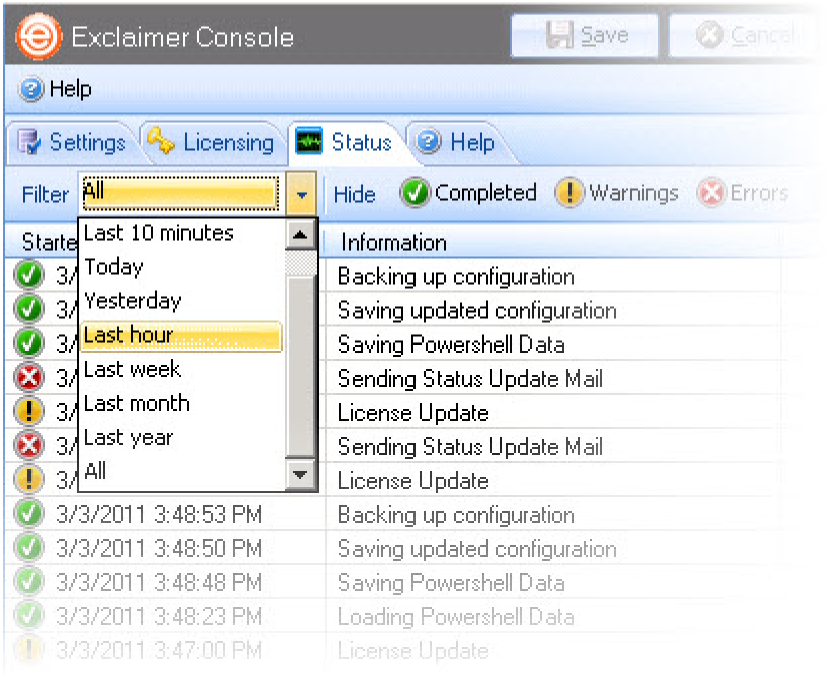
- Filtering the status list [pg.46]
- The status toolbar [pg.48]
- Actions [pg.48]

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

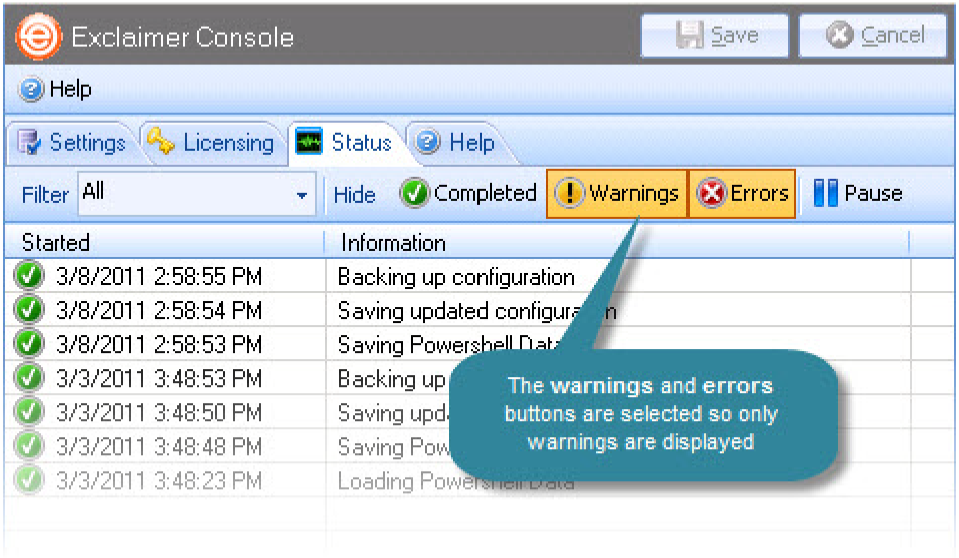
Use the drop-down filter list to select a time period. Having made your selection, the status list is updated to show only items that occurred within that time period:



Started	Information
3/	Backing up configuration
3/	Saving updated configuration
3/	Saving Powershell Data
3/	Sending Status Update Mail
3/	License Update
3/	Sending Status Update Mail
3/	License Update
3/3/2011 3:48:53 PM	Backing up configuration
3/3/2011 3:48:50 PM	Saving updated configuration
3/3/2011 3:48:48 PM	Saving Powershell Data
3/3/2011 3:48:23 PM	Loading Powershell Data
3/3/2011 3:47:00 PM	License Update

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:

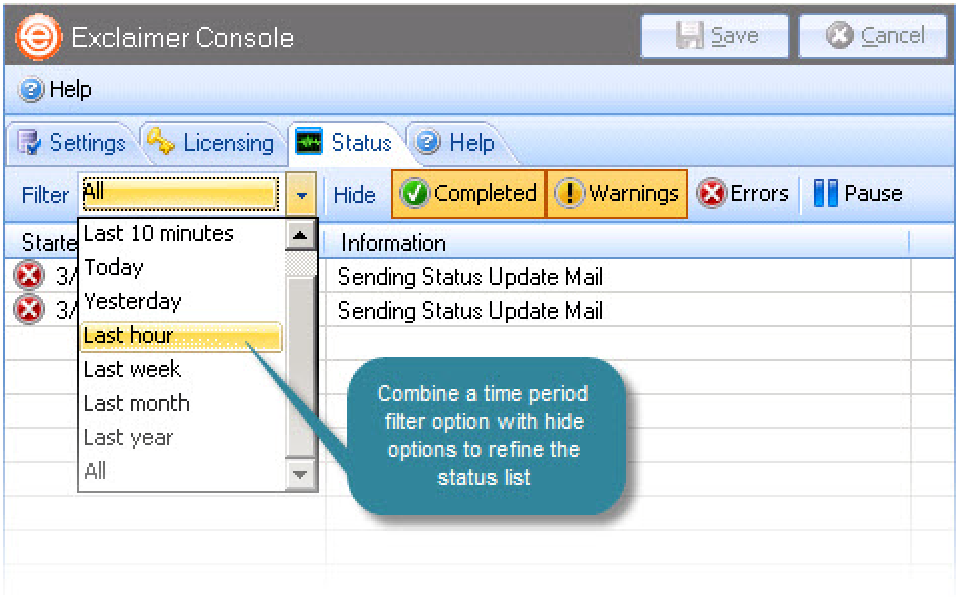


Started	Information
3/8/2011 2:58:55 PM	Backing up configuration
3/8/2011 2:58:54 PM	Saving updated configura n
3/8/2011 2:58:53 PM	Saving Powershell Dat
3/3/2011 3:48:53 PM	Backing up
3/3/2011 3:48:50 PM	Saving upd
3/3/2011 3:48:48 PM	Saving Pow
3/3/2011 3:48:23 PM	Loading Powershell Data

The **warnings** and **errors** buttons are selected so only warnings are displayed

Filter by Time Period and Category

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



Starte	Information
3/	Sending Status Update Mail
3/	Sending Status Update Mail

Combine a time period filter option with hide options to refine the status list

The Status Toolbar

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

Toolbar Option	Summary
Help	Display help for the status window.

Actions

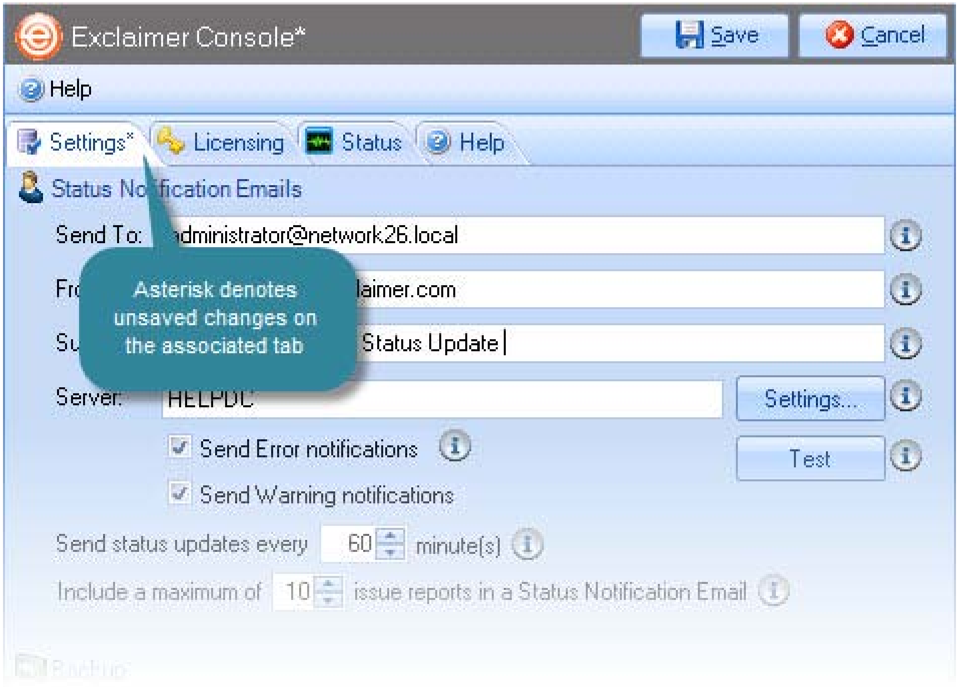
The following actions are available from the status tab:

Action	Select this option to...
System	
Export configuration...	Export all settings - see the export configuration... [pg.51] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [pg.52] page.
Licensing	Access the licensing tab to view licensing information [pg.42].
Anti Spam	
Status	View status information [pg.45] for Exclaimer Anti-spam.
Refresh data	Refresh the current configuration with anti-spam settings from Exchange. Note that any unsaved changes will be lost if you perform a refresh.

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 (see page 49) across all tabs. Alternatively, use the **cancel** button to abandon all changes.

Saving Changes in the Exclaimer Console

If a tab contains any unsaved changes (irrespective of which branch in the console tree [pg.34] is active), it is displayed with an asterisk (*) symbol - for example:



Status Notification Emails

Send To: administrator@network26.local

From: ...laimer.com

Subject: ... Status Update

Server: HELPDC

☑ Send Error notifications

☑ Send Warning notifications

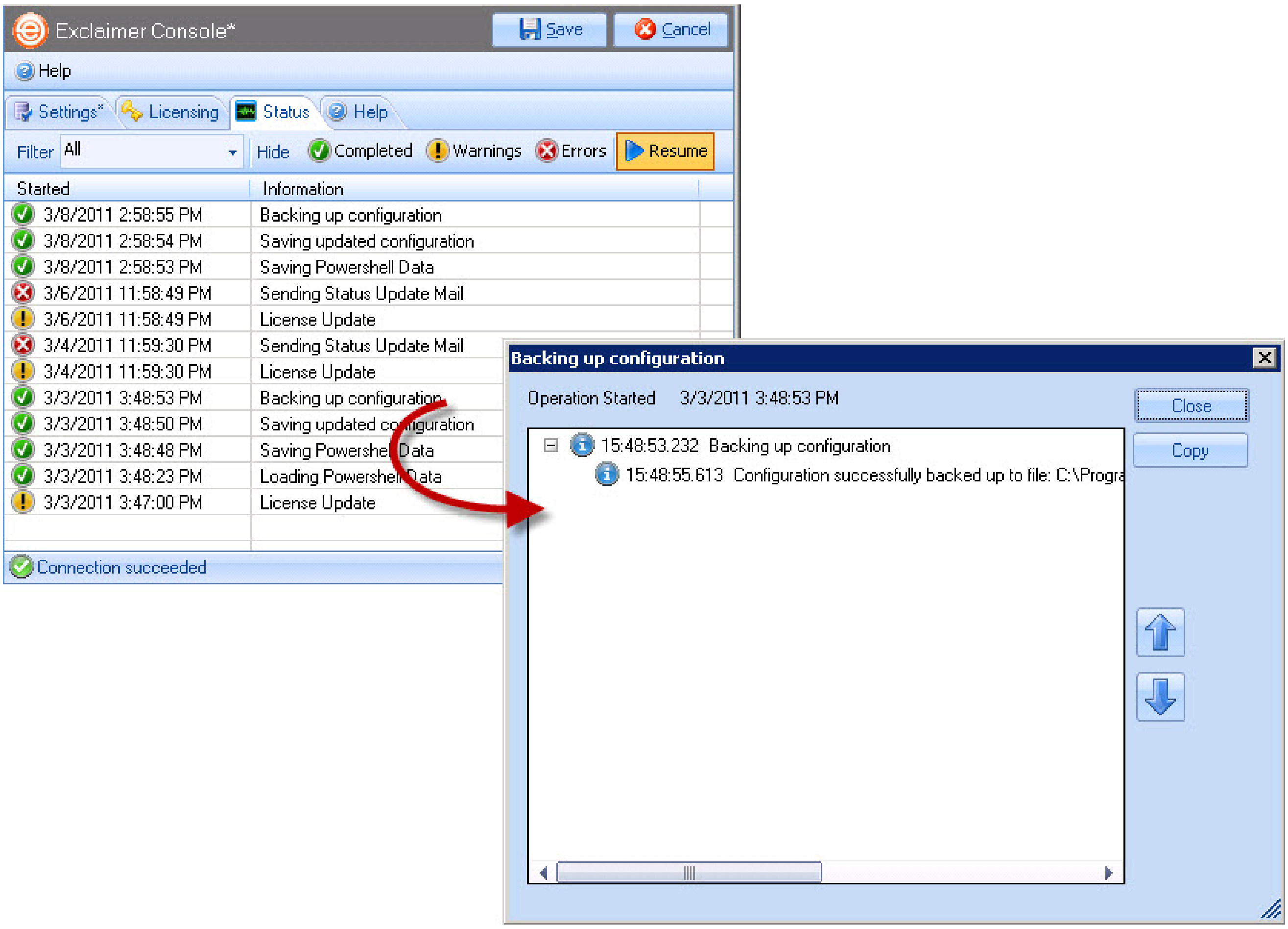
Send status updates every 60 minute(s)

Include a maximum of 10 issue reports in a Status Notification Email

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

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 [pg.45] for the Exclaimer console:



Started	Information
✓ 3/8/2011 2:58:55 PM	Backing up configuration
✓ 3/8/2011 2:58:54 PM	Saving updated configuration
✓ 3/8/2011 2:58:53 PM	Saving Powershell Data
✗ 3/6/2011 11:58:49 PM	Sending Status Update Mail
! 3/6/2011 11:58:49 PM	License Update
✗ 3/4/2011 11:59:30 PM	Sending Status Update Mail
! 3/4/2011 11:59:30 PM	License Update
✓ 3/3/2011 3:48:53 PM	Backing up configuration
✓ 3/3/2011 3:48:50 PM	Saving updated configuration
✓ 3/3/2011 3:48:48 PM	Saving Powershell Data
✓ 3/3/2011 3:48:23 PM	Loading Powershell Data
! 3/3/2011 3:47:00 PM	License Update

✓ Connection succeeded

Backing up configuration

Operation Started 3/3/2011 3:48:53 PM

```
⊟ 15:48:53.232  Backing up configuration
    15:48:55.613  Configuration successfully backed up to file: C:\Progra
```

Once you have chosen to display information for an entry in the status list, you can use up/down arrow buttons to step through details for previous/next entries in the list. This is quicker than closing the details window and selecting another entry from the status list.

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 rules [pg.63] and features [pg.120] for Exclaimer Anti-spam.

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 rules [pg.63] and features [pg.120] for Exclaimer Anti-spam.

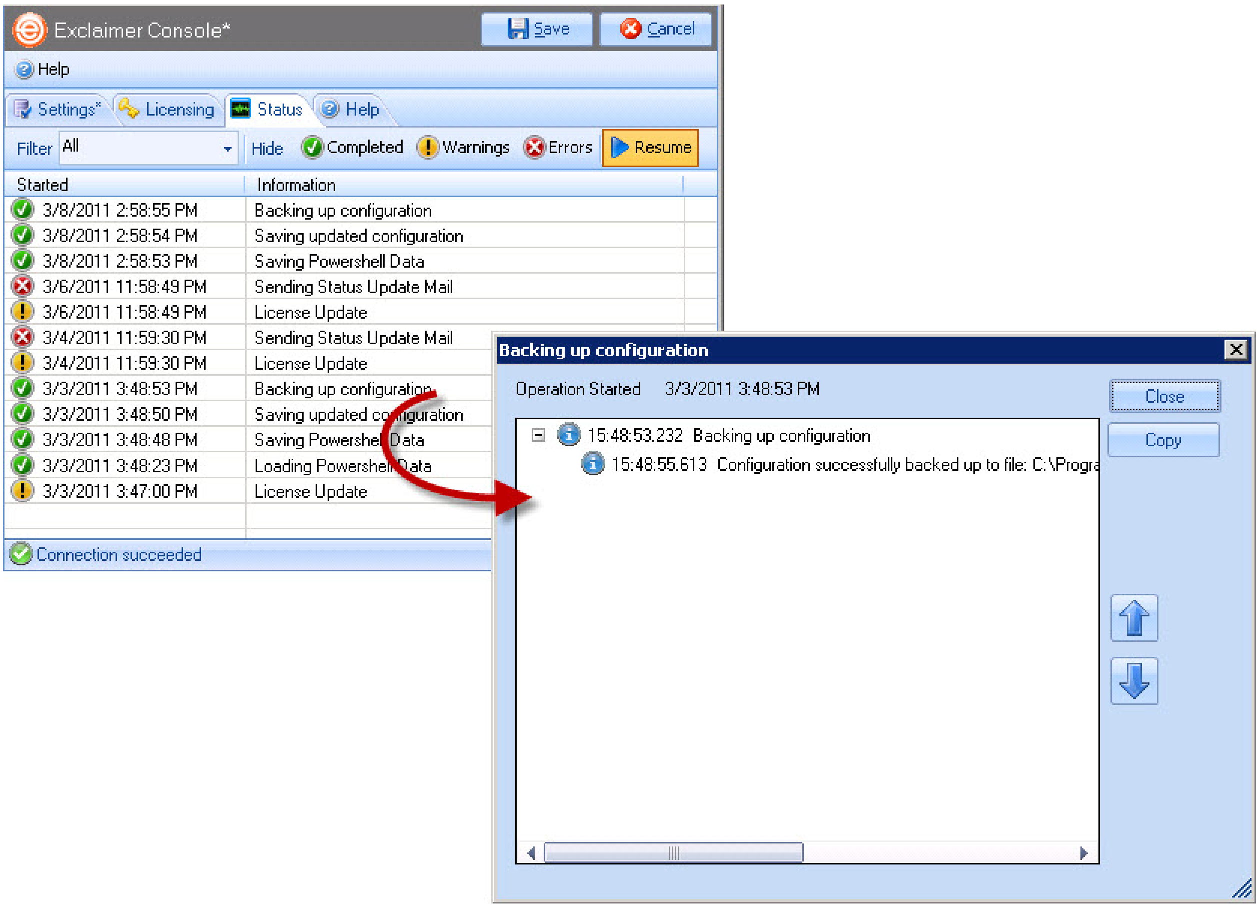
Settings must be imported from an econfig file; this is a proprietary file type for Exclaimer products, and is created whenever the export configuration settings [pg.51] option is used. To import configuration settings, follow the steps below:

1. Ensure that you have backed up existing settings by exporting the current configuration [pg.51].
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.

Backing up Existing Settings Prior to 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 [pg.45] for the Exclaimer console:



Started	Information
3/8/2011 2:58:55 PM	Backing up configuration
3/8/2011 2:58:54 PM	Saving updated configuration
3/8/2011 2:58:53 PM	Saving Powershell Data
3/6/2011 11:58:49 PM	Sending Status Update Mail
3/6/2011 11:58:49 PM	License Update
3/4/2011 11:59:30 PM	Sending Status Update Mail
3/4/2011 11:59:30 PM	License Update
3/3/2011 3:48:53 PM	Backing up configuration
3/3/2011 3:48:50 PM	Saving updated configuration
3/3/2011 3:48:48 PM	Saving Powershell Data
3/3/2011 3:48:23 PM	Loading Powershell Data
3/3/2011 3:47:00 PM	License Update

Connection succeeded

Backing up configuration

Operation Started 3/3/2011 3:48:53 PM

```
15:48:53.232  Backing up configuration
    15:48:55.613  Configuration successfully backed up to file: C:\Progra
```

Refreshing Data

Exclaimer Anti-spam provides a layer over existing Microsoft Exchange anti-spam settings - when changes are made in Exclaimer Anti-spam, they will be applied to your Microsoft Exchange configuration.

Conversely, any changes that might be made to anti-spam settings within Microsoft Exchange will be loaded into Exclaimer Anti-spam (either when the software is closed and restarted, or when you choose to refresh data [pg.54] whilst Exclaimer Anti-spam is running).

The refresh data option is available from the actions pane throughout the application. If it is possible that changes have been made to Microsoft Exchange anti-spam settings outside of Exclaimer Anti-spam, it is a good idea to refresh data.

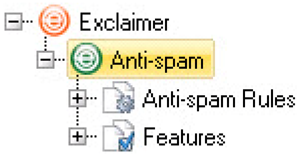
When this option is used, all anti spam features within Microsoft Exchange are refreshed within Exclaimer Anti-spam.

Chapter 4

Exclaimer Anti-spam: General Settings & Information

Introduction

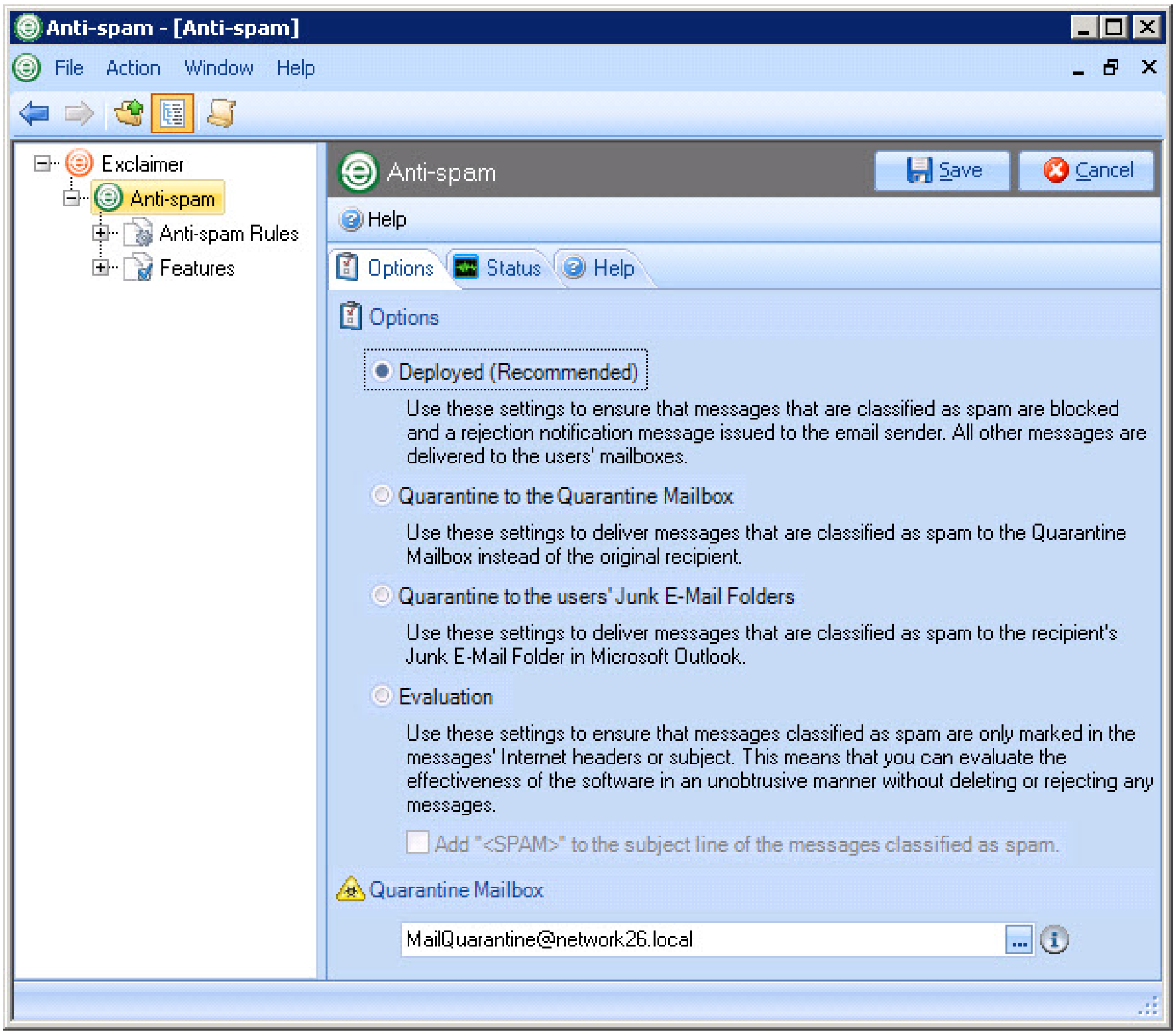
The Anti-spam branch (within the Exclaimer console tree) is where general setup is completed:



Exclaimer Anti-spam controls spam using rules [pg.63] and these rules are based upon features [pg.120]. When the parent branch (Anti-spam) is selected, general settings and information [pg.57] can be viewed and updated. Below this, child branches are used to manage all aspects of rules and features.

General Settings and Information

When the parent branch (Anti-spam) is selected within the Exclaimer console, you can use options [pg.58] to determine how Exclaimer Anti-spam should operate and you can check the status [pg.60] of the application:



● Deployed (Recommended)

Use these settings to ensure that messages that are classified as spam are blocked and a rejection notification message issued to the email sender. All other messages are delivered to the users' mailboxes.

○ Quarantine to the Quarantine Mailbox

Use these settings to deliver messages that are classified as spam to the Quarantine Mailbox instead of the original recipient.

○ Quarantine to the users' Junk E-Mail Folders

Use these settings to deliver messages that are classified as spam to the recipient's Junk E-Mail Folder in Microsoft Outlook.

○ Evaluation

Use these settings to ensure that messages classified as spam are only marked in the messages' Internet headers or subject. This means that you can evaluate the effectiveness of the software in an unobtrusive manner without deleting or rejecting any messages.

□ Add "<SPAM>" to the subject line of the messages classified as spam.

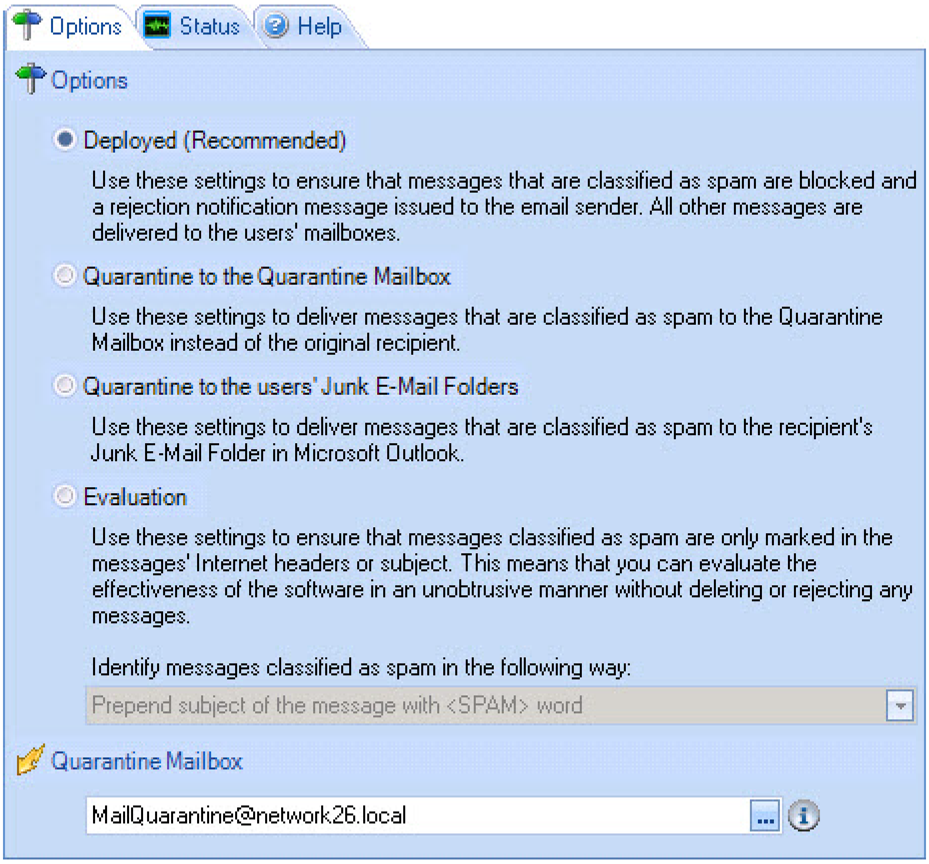
Quarantine Mailbox

MailQuarantine@network26.local

For further information about the Exclaimer console (including the menu, toolbar and actions pane), see understanding the Exclaimer console window on page 34.

Anti-spam Options

When Exclaimer Anti-spam is first installed [pg.21], you are asked to select a scenario - i.e. to select the mode in which Exclaimer Anti-spam should run. Available scenarios can be viewed on the options tab; from here you can see which scenario is currently in use and if required, you can choose a different option:



Options

● Deployed (Recommended)

Use these settings to ensure that messages that are classified as spam are blocked and a rejection notification message issued to the email sender. All other messages are delivered to the users' mailboxes.

○ Quarantine to the Quarantine Mailbox

Use these settings to deliver messages that are classified as spam to the Quarantine Mailbox instead of the original recipient.

○ Quarantine to the users' Junk E-Mail Folders

Use these settings to deliver messages that are classified as spam to the recipient's Junk E-Mail Folder in Microsoft Outlook.

○ Evaluation

Use these settings to ensure that messages classified as spam are only marked in the messages' Internet headers or subject. This means that you can evaluate the effectiveness of the software in an unobtrusive manner without deleting or rejecting any messages.

Identify messages classified as spam in the following way:

Prepend subject of the message with <SPAM> word

Quarantine Mailbox

MailQuarantine@network26.local

Each deployment scenario is associated a set of predefined options. When a scenario is selected, Exclaimer Anti-spam's features [pg.120] and rules [pg.63] are automatically reset to apply these options. Available scenarios are:

- Deployed [pg.59]
- Quarantine to the Quarantine Mailbox [pg.59]
- Quarantine to the users' junk e-mail folder [pg.59]
- Evaluation [pg.59]
- Custom [pg.59]

These options are summarized in the following sections.

Deployed Mode

When the deployed option is selected, Exclaimer Anti-spam will reject any messages which are classified as spam. A notification email message is sent to the sender to advise that their message has been rejected and the recipient is unaware that the message was ever sent to them. This is the recommended mode of operation.

Quarantine to Quarantine Mailbox

When the quarantine to Quarantine Mailbox option is selected, Exclaimer Anti-spam will redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is set at the bottom of this tab.

Quarantine to the Users' Junk E-mail Folder

When the quarantine to the users' junk e-mail folder option is selected, Exclaimer Anti-spam will deliver messages which are classified as spam to the recipient(s). However, these messages will be redirected to the users' junk e-mail folder in Microsoft Outlook.

Evaluation Mode

When the evaluation option is selected, Exclaimer Anti-spam does not block messages which are classified as spam. Instead, these messages are identified as spam and then delivered to the intended recipient(s). When running in evaluation mode, you can choose to:

- Insert the text <SPAM> at the start of the message subject line. This means that recipients can clearly see if a message has been classified as spam.

  -or-

- Add an Internet header [X-EXCLAIMER-SPAM] to the message.

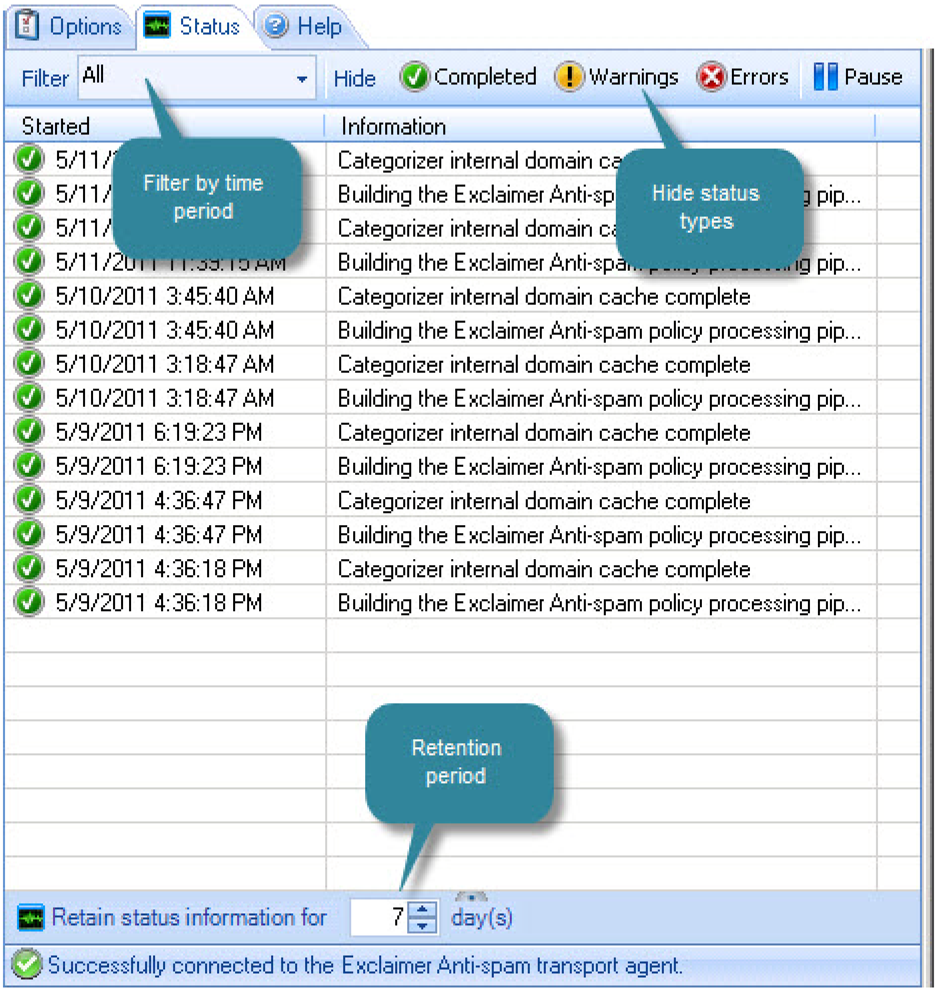
Custom

If you change any Exclaimer Anti-spam features [pg.120] or rules [pg.63] (with the exception of adding/updating entries in white/block lists), the deployed scenario is automatically changed to custom. If you have made changes and wish to revert to a standard deployment scenario, you can simply select one of the options described above.

If you do revert to a standard scenario, any changes made to your white/block lists will **not** be affected however, any changes made to features will be cleared and reset to default values. **If you are in any doubt, please contact support** [pg.9] **before resetting the deployment mode**.

Anti-spam Status

The status tab contains information and actions [pg.61] regarding activity within Exclaimer Anti-spam. Double click an entry in the list to view further details. Entries are categorised as completed, warnings or errors, as shown below:



Started	Information
✓ 5/11/	Categorizer internal domain ca
✓ 5/11/	Building the Exclaimer Anti-sp pip...
✓ 5/11/	Categorizer internal domain ca
✓ 5/11/2011	Building the Exclaimer Anti-spam ng pip...
✓ 5/10/2011 3:45:40 AM	Categorizer internal domain cache complete
✓ 5/10/2011 3:45:40 AM	Building the Exclaimer Anti-spam policy processing pip...
✓ 5/10/2011 3:18:47 AM	Categorizer internal domain cache complete
✓ 5/10/2011 3:18:47 AM	Building the Exclaimer Anti-spam policy processing pip...
✓ 5/9/2011 6:19:23 PM	Categorizer internal domain cache complete
✓ 5/9/2011 6:19:23 PM	Building the Exclaimer Anti-spam policy processing pip...
✓ 5/9/2011 4:36:47 PM	Categorizer internal domain cache complete
✓ 5/9/2011 4:36:47 PM	Building the Exclaimer Anti-spam policy processing pip...
✓ 5/9/2011 4:36:18 PM	Categorizer internal domain cache complete
✓ 5/9/2011 4:36:18 PM	Building the Exclaimer Anti-spam policy processing pip...

Retain status information for 7 day(s)

✓ Successfully connected to the Exclaimer Anti-spam transport agent.

Filter by time period

Hide status types

Retention period

Available options are summarized in the following sections:

- Filtering the status list [pg.61]
- Actions [pg.61]

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 completed entries, you would click hide buttons for warnings and errors categories.

Filter by Time Period and Status Type

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

For more detailed information about using these filter options please refer to the Exclaimer console status section [pg. 45] of this guide.

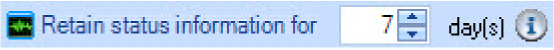
Actions

The following actions are available from the status tab:

Action	Select this option to...
System	
Export configuration...	Export all settings - see the export configuration... [pg.51] page.
Import configuration...	Import a previously exported configuration file - see the import configuration... [pg.52] page.
Licensing	Access the licensing tab to view licensing information [pg.42].
Anti Spam	
Status	View status information [pg.45] for Exclaimer Anti-spam.
Refresh data	Refresh the current configuration with anti-spam settings from Exchange. Note that any unsaved changes will be lost if you perform a refresh.

Status Information Retention

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



Retain status information for 7 day(s)

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

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 (see page 49) across all tabs. Alternatively, use the **cancel** button to abandon all changes.

Chapter 5

Exclaimer Anti-spam: Rules

Introduction

Within Exclaimer Anti-spam, rules provide straightforward, intuitive access to anti-spam settings that are likely to be changed on a more regular basis. They are also used to define additional 'belt and braces' options which are specific to Exclaimer Anti-spam and provide an extra level of security.

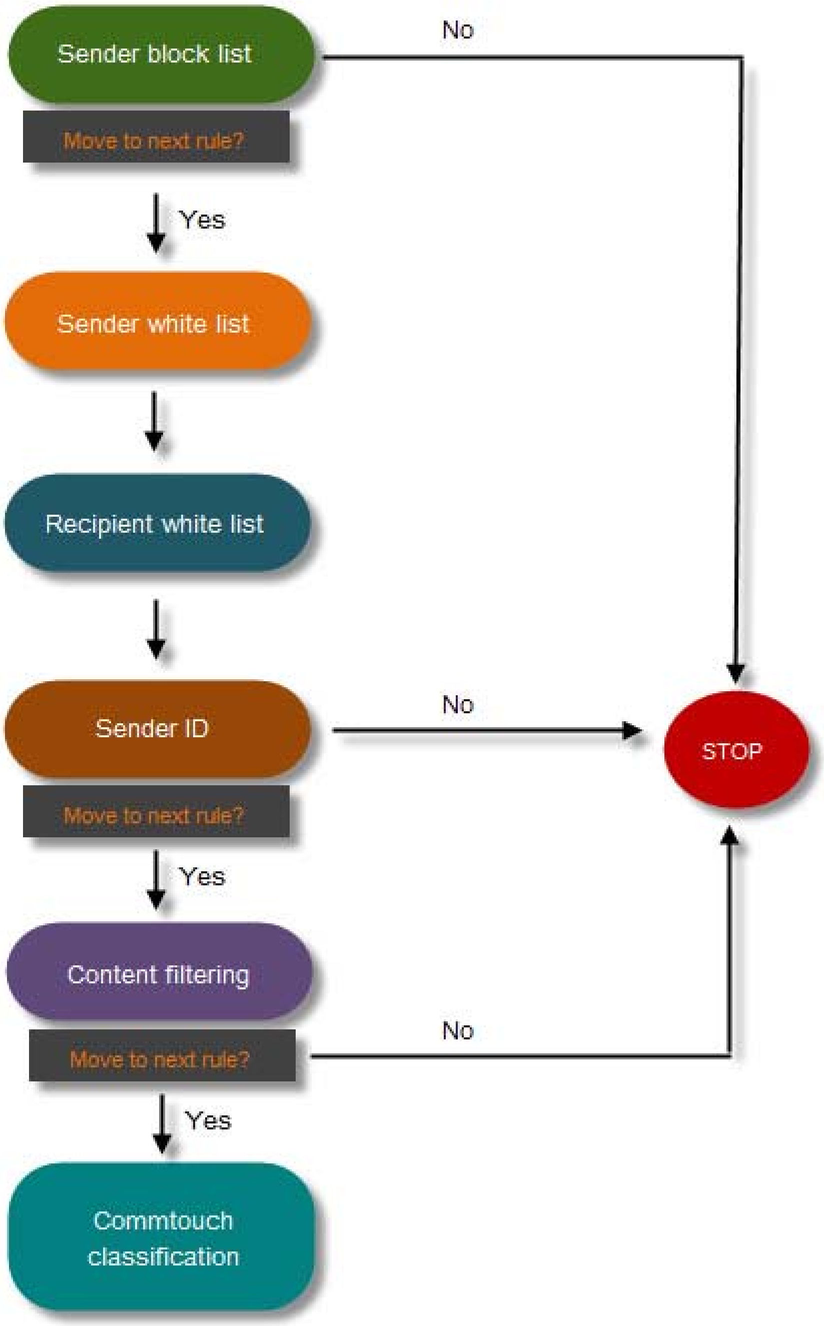
When Exclaimer Anti-spam is running, rules are processed **after** features [pg.120] in the anti-spam chain. In practice, you are unlikely to update features on more than an occasional basis, but you might change rules more regularly to meet the specific needs of your organization.

Rules are processed in the same sequence that they appear in the console tree - namely:

Rule	Summary
Sender block list	Maintain a list of email addresses and/or email domains which are known to send spam email messages. For further information please see page 67.
Sender white list	Maintain a list of email addresses and/or email domains which are considered to be 'safe'. For further information please see page 77.
Recipient white list	Maintain a list of email addresses within your organisation for which anti-spam rules should **not** be applied. For further information please see page 84.
Sender ID	Specify what actions should be taken with messages which are given different Sender Policy Framework (SPF) results as a result of sender ID checking. For further information please see page 89.
Content filtering	Specify what actions should be taken with messages at given Spam Confidence Level (SCL) thresholds. For further information please see page 100.
Commtouch classifications	Specify what action should be taken with email messages which are given different Commtouch classifications. For further information please see page 106.

The processing sequence cannot be changed however, in some cases you can choose to stop processing if actions for a rule are applied. For example, if the sender block list [pg.67] rule identifies a message from a blocked contact and is set to reject associated messages; it is not possible to process subsequent rules because message delivery has already been stopped.

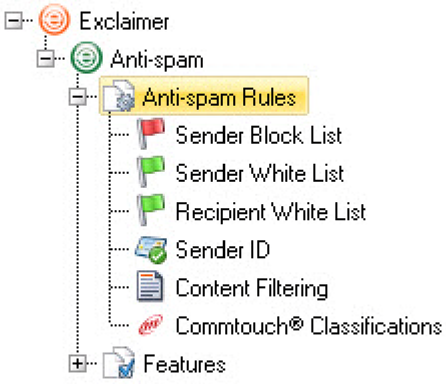
The following illustration shows how the sequence of Exclaimer Anti-spam rules and how certain types of rule can terminate further processing:



Changing **rules** may set your deployment mode [pg.58] to **custom**. If you have made changes and wish to revert to a standard deployment mode, you can simply select one of the standard options. If you do revert to a standard mode of deployment, any changes made to your white/block list **rules** will **not** be affected. However, any changes made to features [pg.119] will be cleared and reset to default values.

Accessing Existing Rules

Within Exclaimer Anti-spam, rules are accessed from the Anti-spam rules branch of the Exclaimer console tree [pg.34]:



From here, all existing rules are displayed; you can select any rule to display information and options. Available rules include:

- Sender block list [pg.67]
- Sender white list [pg.77]
- Recipient white list [pg.84]
- Sender ID [pg.89]
- Content filtering [pg.100]
- Commtouch classifications [pg.106]

Sender Block List

The sender block list is used to maintain a list of email addresses and/or email domains which are known to send spam email messages. Having added names to this list, you can set sender block list options to determine what action should be taken with email messages received from these senders, and what should happen after these actions have been taken.

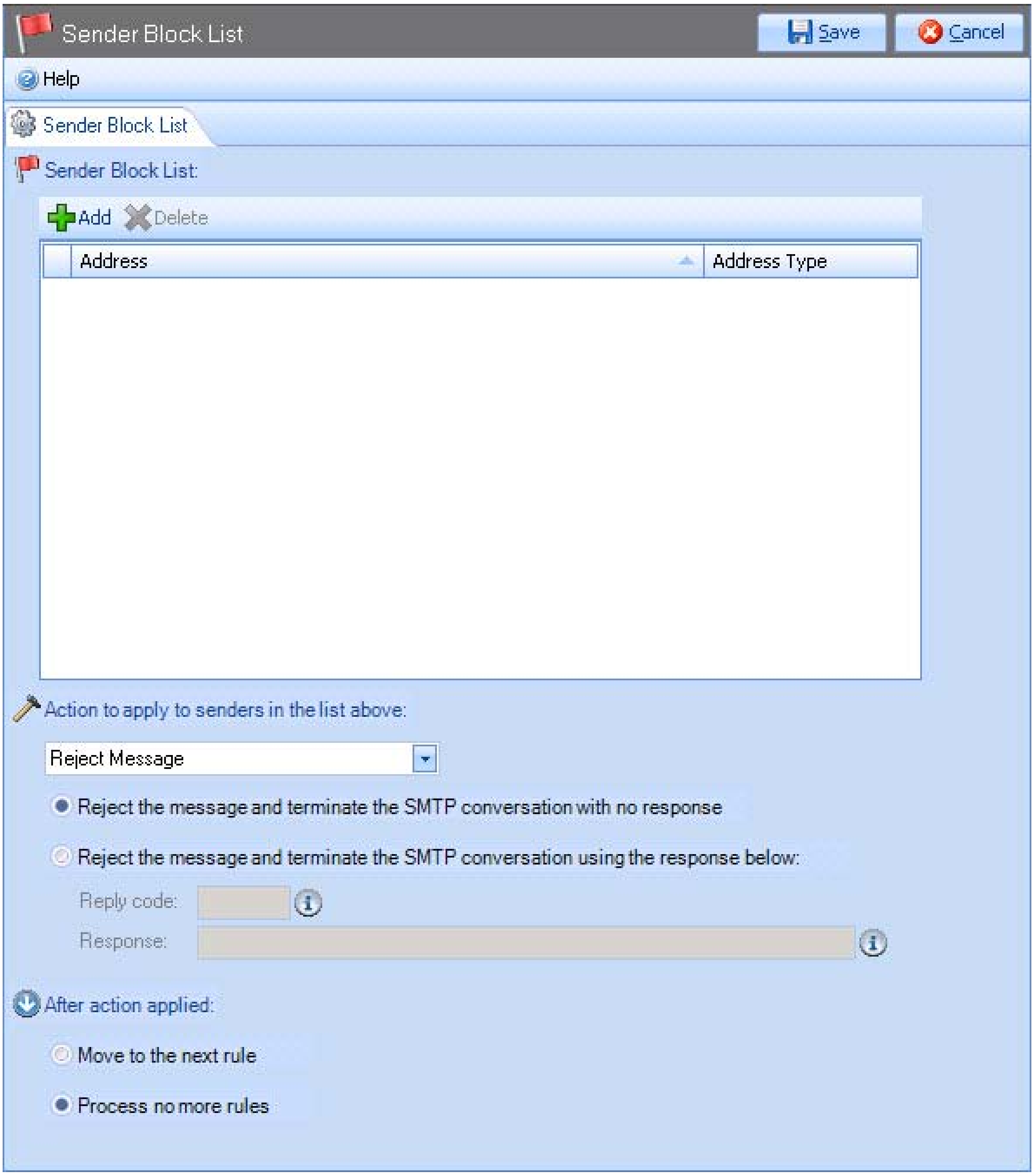
For further information please refer to the following sections:

- Understanding the sender block list window [pg.68]
- Sender block list options [pg.69]
- Adding senders to the sender block list [pg.73]
- Deleting senders from the sender block list [pg.76]

The **sender block list** rule will only be applied if the IP block list feature [pg.132] is enabled.

Understanding the Sender Block List Window

The sender block list window displays email addresses and domains which are considered to be 'unsafe' - i.e. which are known to send spam email messages. Beneath this list, a number of options can be set to determine what action should be taken when email messages are received from addresses or domains in the block list:



Reject Message

● Reject the message and terminate the SMTP conversation with no response

○ Reject the message and terminate the SMTP conversation using the response below:

Reply code:

Response:

After action applied:

○ Move to the next rule

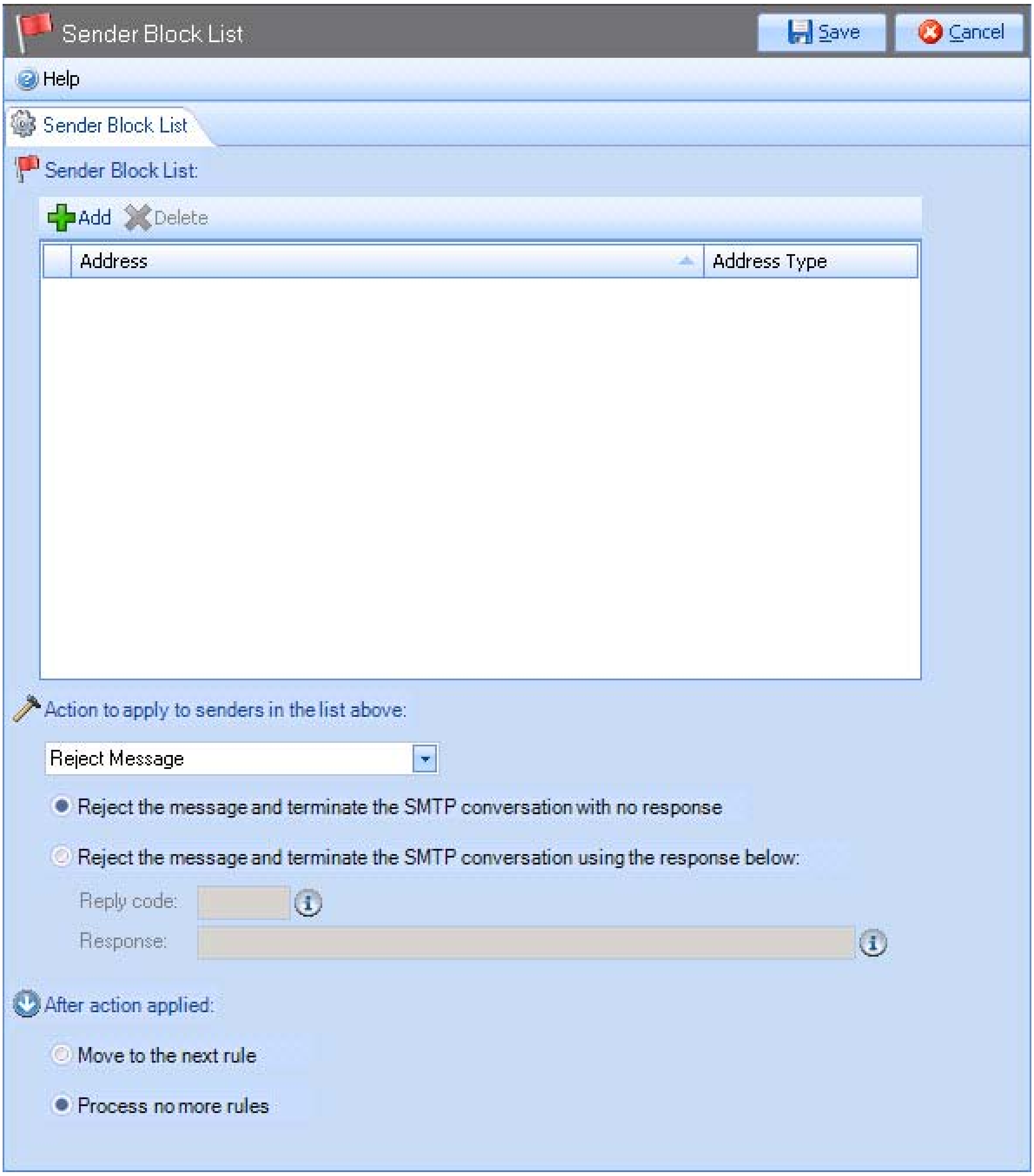
● Process no more rules

You can add a new entry [pg.73] or you can delete an existing entry [pg.76]. For further information about actions to be taken with email messages received from addresses or domains in the block list, see sender block list options [pg.69].

If an email address or domain name has been entered incorrectly (or has been changed) you should delete the entry [pg.76] and add a new entry [pg.73] for the required address.

Sender Block List Options

When you are working with the sender block list, a number of options are available which allow you to specify what happens to email messages that are received from blocked addresses and domains:



Address	Address Type

Action to apply to senders in the list above:

Reject Message

● Reject the message and terminate the SMTP conversation with no response

○ Reject the message and terminate the SMTP conversation using the response below:

Reply code:

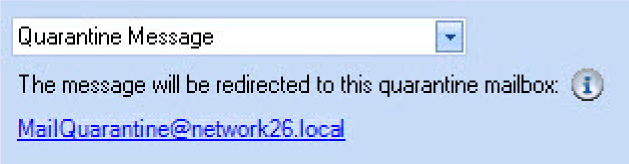
Response:

After action applied:

○ Move to the next rule

● Process no more rules

These options apply to all addresses and domains in the sender block list, as summarized on the following page.

Option	Summary
Action to apply to senders in the list above	
Use the drop-down list to select the required action to be taken with received messages. Subsequent options may be displayed, dependent upon which entry is selected from this list.	
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.
Reject message	Select this option to reject the message, then set additional options as follows: • Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. • Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response Whilst the reply code uses a standard number and text, the response field allows you to enter additional text to be inserted in the message.

.../continued

Option	Summary
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: • Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. • Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value. • Alter subject line. Choose this option if you wish to modify the subject line of email messages received from blocked senders. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows: Modify subject... – Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message. Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message. Replace subject with... – Select this option and specify text to be used instead of the original subject line of the email message. If required you can choose to modify a combination of SCL, Internet header and subject line options.

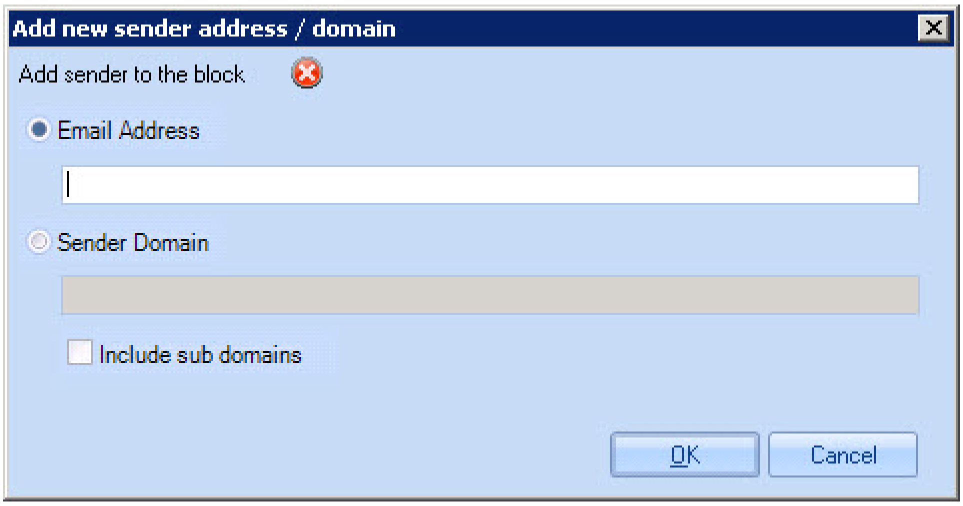
.../continued

Option	Summary
After action applied...	
Move to next rule	Rules are processed in the same sequence that they appear in the console tree - namely: ● Recipient white list [pg.84] ● Sender white list [pg.77] ● Sender block list [pg.67] ● Content filtering [pg.100] ● Sender ID [pg.89] ● Commtouch classifications [pg.106] Select this option if you wish to continue processing rules (i.e. continue to content filtering [pg.100] checks) after specified actions have been applied to email messages from a blocked sender, select this option.
Process no more rules	If you wish to stop processing rules after specified actions have been applied to email messages from a blocked sender, select this option. If you have chosen to reject messages [pg.70] from blocked senders, it is logical to select the **process no more rules** option. However, if you have chosen another action, it is more likely (though not mandatory) that you will want to **move to the next rule**.

Adding Senders to the Sender Block List

When adding entries to the sender block list, you can choose to add individual email addresses, or you can specify a sender domain [pg.74]. To add a new entry, follow the steps below:

1. Expand the Anti-spam rules branch of the Exclaimer console tree [pg.34].
2. Select the sender block list branch to display the sender block list window.
3. Click the add button to open the add new sender address window:



Add new sender address / domain

Add sender to the block

● Email Address

○ Sender Domain

□ Include sub domains

4. If you wish to add a specific email address, select the email address radio button and type the full address (e.g. joe.bloggs@knownspam.com) into the associated field.

   You do not need to worry about adding duplicate entries to the **sender block list**. When an email address is added the system checks to see if it already exists and, if the address is found, it is not added again.

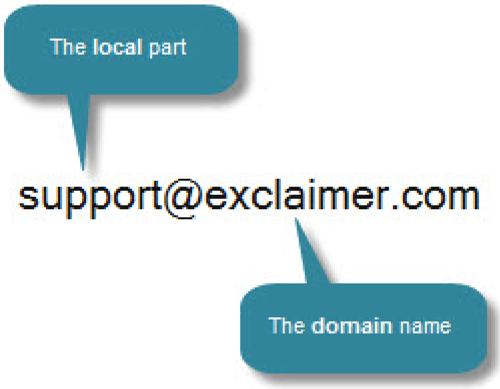
   -or-

   If you wish to add a domain, select the sender domain radio button and type the domain (e.g. knownspam.com) into the associated field. For further information about domains please see the domain information [pg.74] section of this section.

5. If you have chosen to add a sender domain, choose whether or not you wish to include sub domains [pg.75].
6. Click OK to add the entry to the list exit back to the sender block list window.
7. Add further addresses as required.
8. Click the save button (at the top of the window) to save changes.

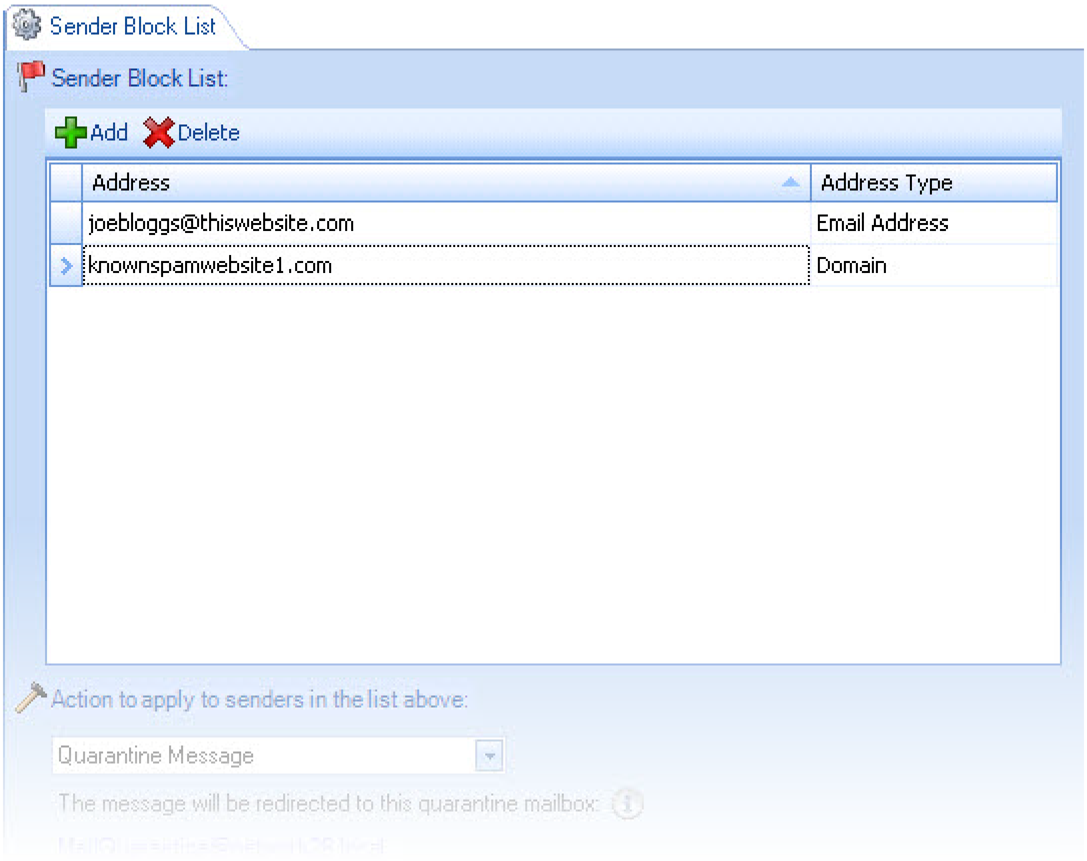
Domain Information

A typical email address looks similar to the example below:



The part before the @ symbol is known as the local part (commonly the username of the recipient) and the part after the @ symbol is the domain name. If you choose to add a sender domain rather than a specific email address, you only need to enter the domain name - i.e. any information after the @ symbol.

It is not necessary to include the @ symbol when specifying a sender domain:



Sender Block List:

	Address	Address Type
	joebloggs@thiswebsite.com	Email Address
>	knownspamwebsite1.com	Domain

Action to apply to senders in the list above:

Quarantine Message

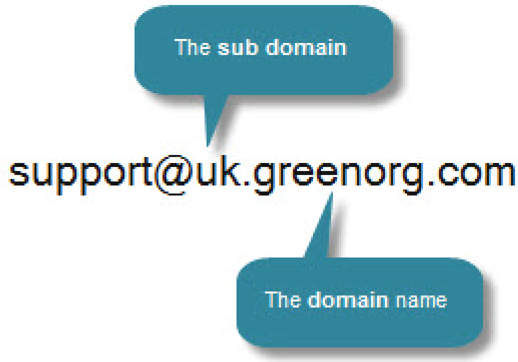
The message will be redirected to this quarantine mailbox:

[illegible]

Sub Domains

When adding a sender domain to the sender block list, you can choose whether or not to include sub domains.

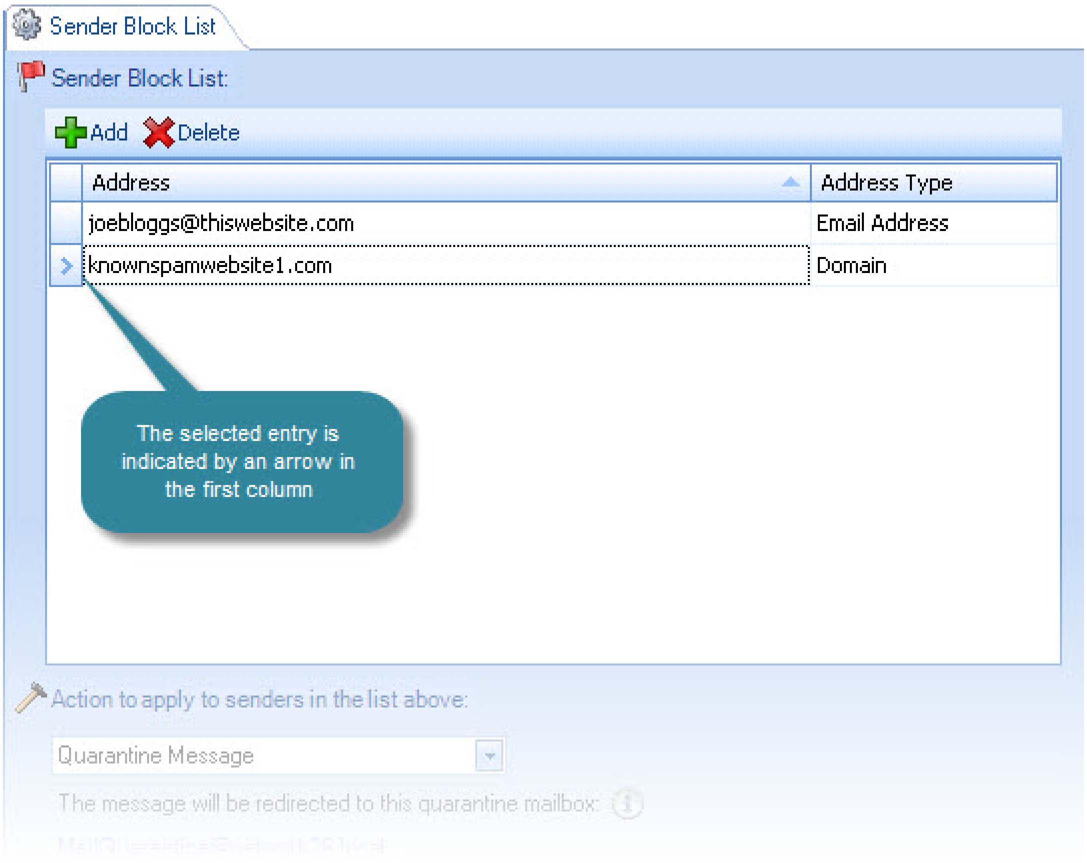
A sub domain is a domain which is part of a larger domain. Sub domains are used for a variety of reasons, one of the most common being to organize functions or information within an organization. For example, the address below shows a sub domain of uk within the main domain of greenorg.com:



Deleting Senders from the Sender Block List

To remove an address from the sender block list, follow the steps below:

1. Expand the Anti-spam rules branch of the Exclaimer console tree [pg.34].
2. Select the sender block list branch to display the sender block list window.
3. Select the entry that you wish to delete:



	Address	Address Type
	joebloggs@thiswebsite.com	Email Address
>	knownspamwebsite1.com	Domain

The selected entry is indicated by an arrow in the first column

Action to apply to senders in the list above:

Quarantine Message

The message will be redirected to this quarantine mailbox:

MailQuarantine@[illegible]

4. Click the delete button. You are asked if you are sure that the selected entry should be removed.
5. If you are satisfied that the correct entry has been selected, click yes to remove the entry and exit back to the sender block list window.
6. Click the save button (at the top of the window) to save changes.

Sender White List

The sender white list is used to maintain a list of email addresses and/or email domains which are considered to be 'safe'. When email messages are received from these senders, specified anti-spam rules [pg.63] will **not** be performed.

For further information please refer to the following sections:

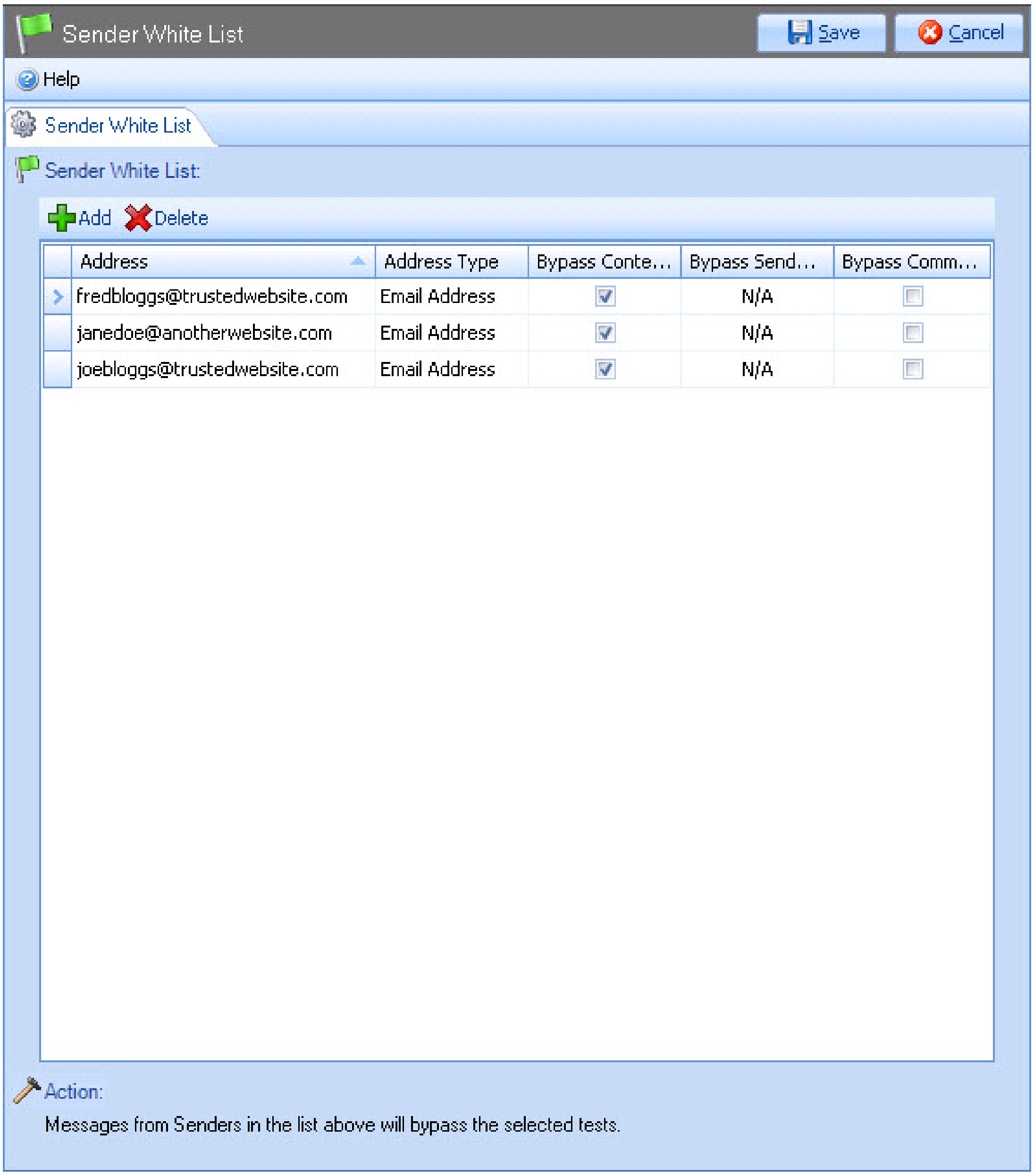
- Understanding the sender white list window [pg.78]
- Adding senders to the sender white list [pg.80]
- Updating sender white list settings [pg.82]
- Deleting senders from the sender white list [pg.83]

The **sender white list** rule will only be applied if the IP allow list feature [pg.123] is enabled.

Understanding the Sender White List Window

The sender white list window displays email addresses and domains which are considered to be 'safe'. Each entry is associated with an email address (or a domain name) together with required white list settings. When an email message is received from an address (or domain) which is on the sender white list, specified anti-spam checks are bypassed.

For each entry in the sender white list, you can choose to enforce or bypass any of the available anti-spam rules, as shown below:



	Address	Address Type	Bypass Conte...	Bypass Send...	Bypass Comm...
>	fredbloggs@trustedwebsite.com	Email Address	☑	N/A	□
	janedoe@anotherwebsite.com	Email Address	☑	N/A	□
	joebloggs@trustedwebsite.com	Email Address	☑	N/A	□

Action:

Messages from Senders in the list above will bypass the selected tests.

Any applicable anti-spam rules can be checked or unchecked as required. If an option is checked (ticked) it means that the associated rule will **not** be applied to any messages received from this address. You can also add a new entry [pg.80], update settings for an existing entry [pg.82] or you can delete an existing entry [pg.83].

Default Settings

When an email address is added to the sender white list, default settings are that all anti-spam rules are checked (i.e. set to be ignored) except for Commtouch white list.

The default is set in this way because Commtouch [pg.106] checks are considered to be so accurate that it is worth applying this rule under any circumstances. However, this is only a recommended setting and default options can be changed as required.

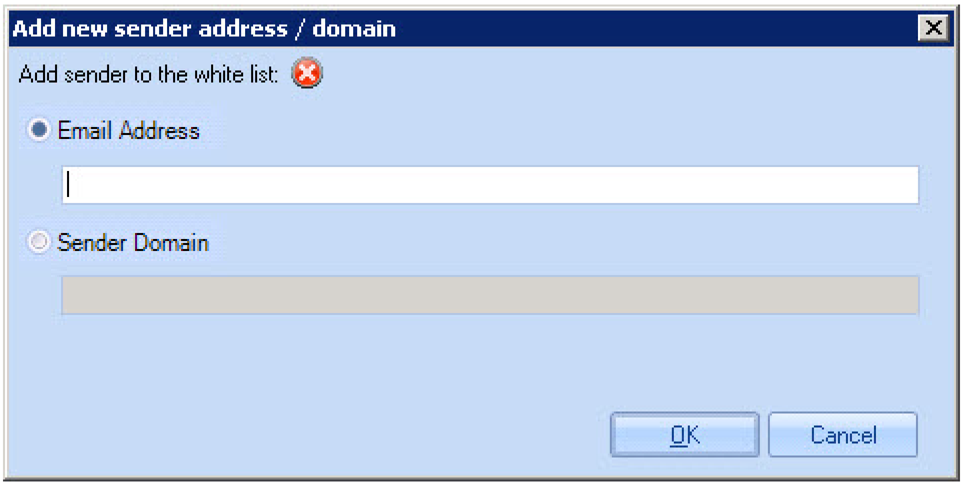
Adding Senders to the Sender White List

When adding entries to the sender white list, you can choose to add individual email addresses or - if you trust all uses for a given organisation - you can specify a sender domain [pg.81]. To add a new entry, follow the steps below:

1. Expand the Anti-spam rules branch of the Exclaimer console tree [pg.34].

2. Select the sender white list branch to display the sender white list window.

3. Click the add button to open the add new sender address window:



Add new sender address / domain

Add sender to the white list:

● Email Address

○ Sender Domain

4. If you wish to add a specific email address, select the email address radio button and type the full address (e.g. joe.bloggs@exclaimer.com) into the associated field.

   You do not need to worry about adding duplicate entries to the **sender white list**. When an email address is added the system checks to see if it already exists and, if the address is found, it is not added again.

   -or-

   If you wish to add a domain, select the sender domain radio button and type the domain (e.g. exclaimer.com) into the associated field. For further information about domains please see the domain information [pg.81] section of this section.

5. Click OK to add the entry to the list exit back to the sender white list window.

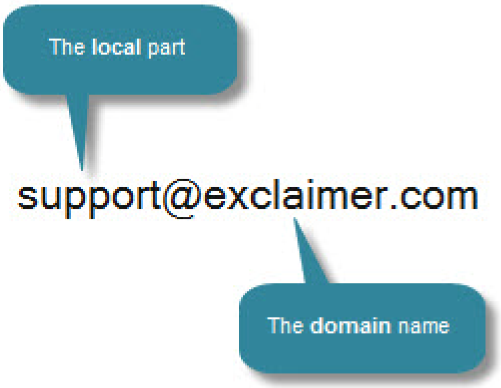
   When an email address is added to the **sender white list**, default settings are that all applicable **Anti-spam** rules are checked (i.e. set to be ignored) except for **Commtouch classifications**.

6. Add further addresses as required.

7. Click the save button (at the top of the window) to save changes.

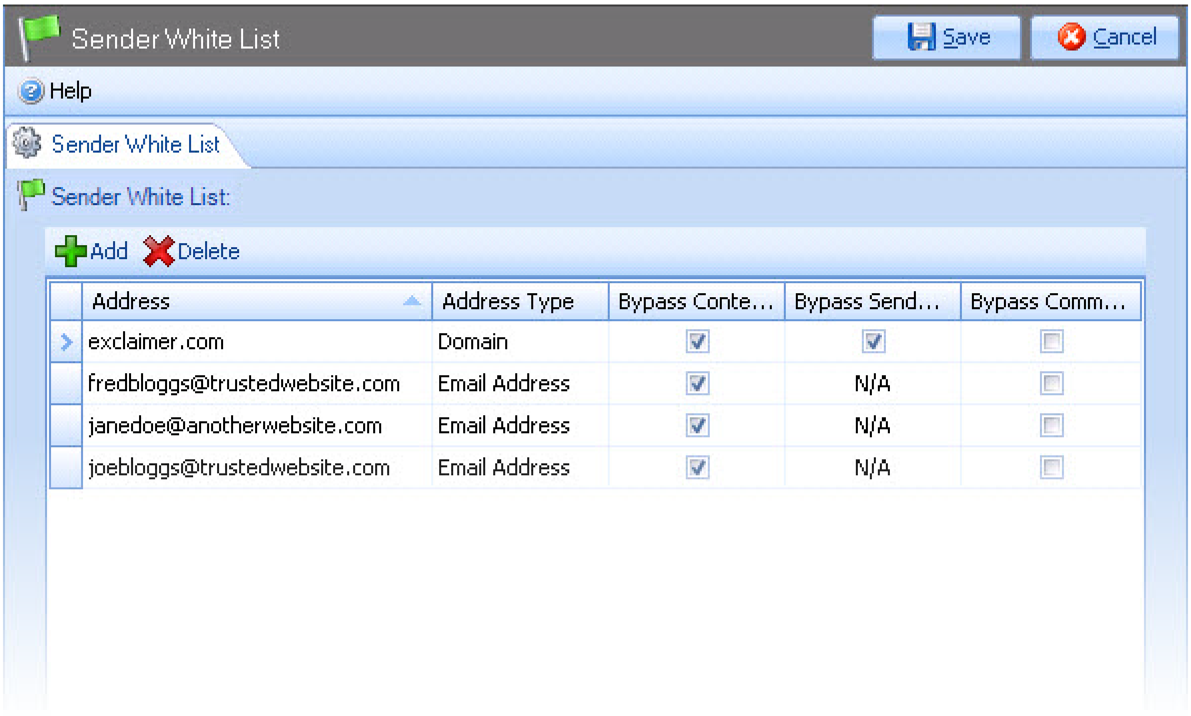
Domain Information

A typical email address looks similar to the example below:



The part before the @ symbol is known as the local part (commonly the username of the recipient) and the part after the @ symbol is the domain name. If you choose to add a sender domain rather than a specific email address, you only need to enter the domain name - i.e. any information after the @ symbol.

It is not necessary to include the @ symbol when specifying a sender domain:

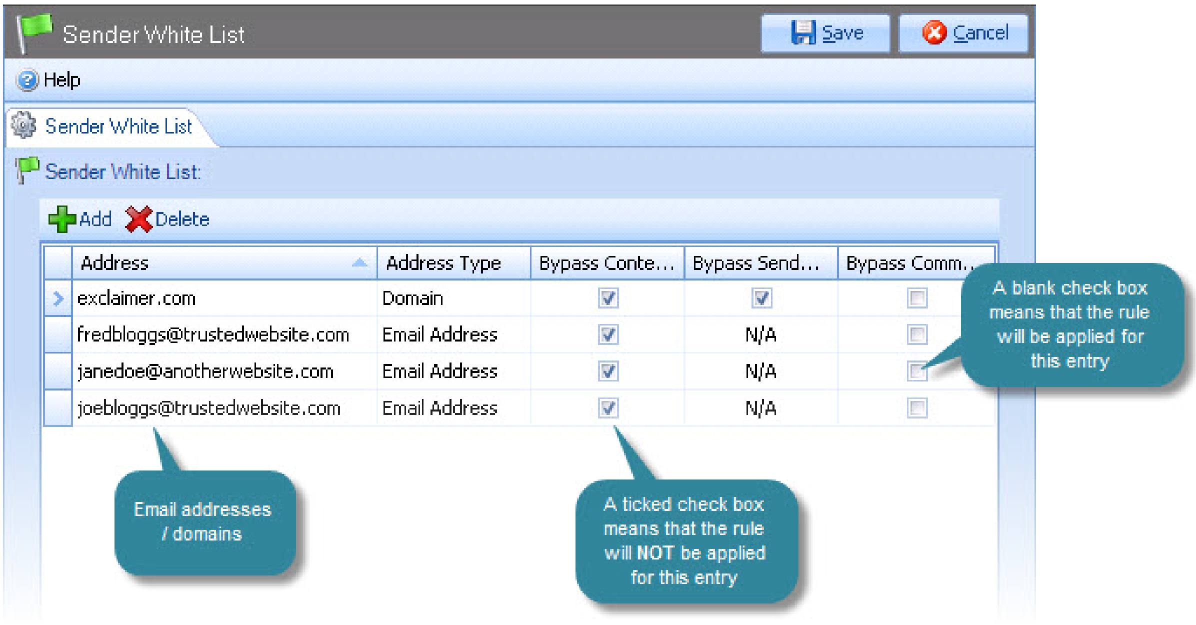


Address	Address Type	Bypass Conte...	Bypass Send...	Bypass Comm...
exclaimer.com	Domain	☑	☑	☐
fredbloggs@trustedwebsite.com	Email Address	☑	N/A	☐
janedoe@anotherwebsite.com	Email Address	☑	N/A	☐
joebloggs@trustedwebsite.com	Email Address	☑	N/A	☐

You will also notice that the sender ID [pg.89] rule bypass option becomes available for selection / de-selection for domain names.

Updating Sender White List Settings

Each entry in the sender white list is associated with an email address or a domain name, together with a series of check boxes that determine which rules (i.e. anti spam checks) are applied for the entry and which rules should not be applied:



Address	Address Type	Bypass Conte...	Bypass Send...	Bypass Comm...
exclaimer.com	Domain	☑	☑	□
fredbloggs@trustedwebsite.com	Email Address	☑	N/A	□
janedoe@anotherwebsite.com	Email Address	☑	N/A	□
joebloggs@trustedwebsite.com	Email Address	☑	N/A	□

A blank check box means that the rule will be applied for this entry

Email addresses / domains

A ticked check box means that the rule will **NOT** be applied for this entry

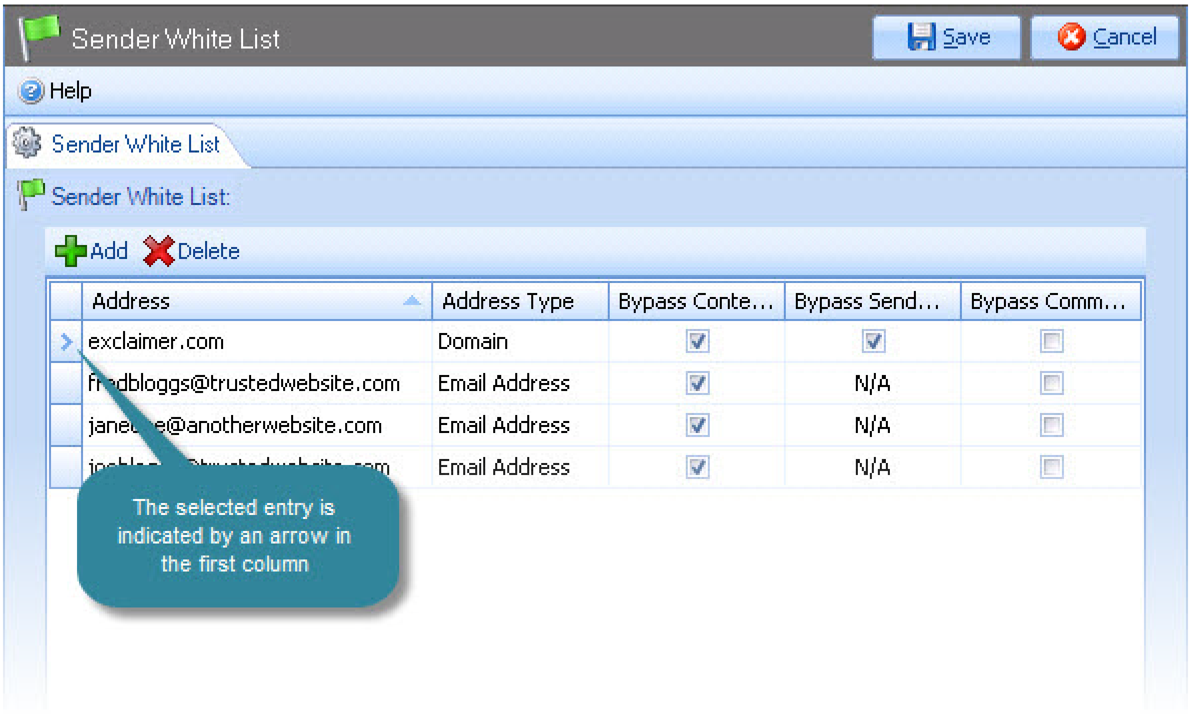
Here, a ticked check box means that the rule will **not** be applied for the associated entry and conversely, a blank check box means that the rule will be applied. If you wish to change these settings for an entry, simply select and de-select associated check boxes as required.

If an email address or domain name has been entered incorrectly (or has been changed) you should delete the entry [pg.83] from the **sender white list** and add a new entry [pg.80] for the required address.

Deleting Senders from the Sender White List

To remove an address from the sender white list, follow the steps below:

1. Expand the Anti-spam rules branch of the Exclaimer console tree [pg.34].
2. Select the sender white list branch to display the sender white list window.
3. Select the entry that you wish to delete:



	Address	Address Type	Bypass Conte...	Bypass Send...	Bypass Comm...
›	exclaimer.com	Domain	☑	☑	□
	fr dbloggs@trustedwebsite.com	Email Address	☑	N/A	□
	jane e@anotherwebsite.com	Email Address	☑	N/A	□
	[illegible]	Email Address	☑	N/A	□

The selected entry is indicated by an arrow in the first column

4. Click the delete button. You are asked if you are sure that the selected entry should be removed.
5. If you are satisfied that the correct entry has been selected, click yes to remove the entry and exit back to the sender white list window.
6. Click the save button (at the top of the window) to save changes.

Recipient White List

The recipient white list is used to maintain a list of email addresses within your organisation for which Exclaimer Anti-spam rules [pg.63] should **not** be performed when email messages are received. For example, you might choose to be less stringent with email that is sent to company managers and directors, or you might have staff who legitimately receive email that could be classified as spam and so wish to exclude them from certain checks.

For further information please refer to the following sections:

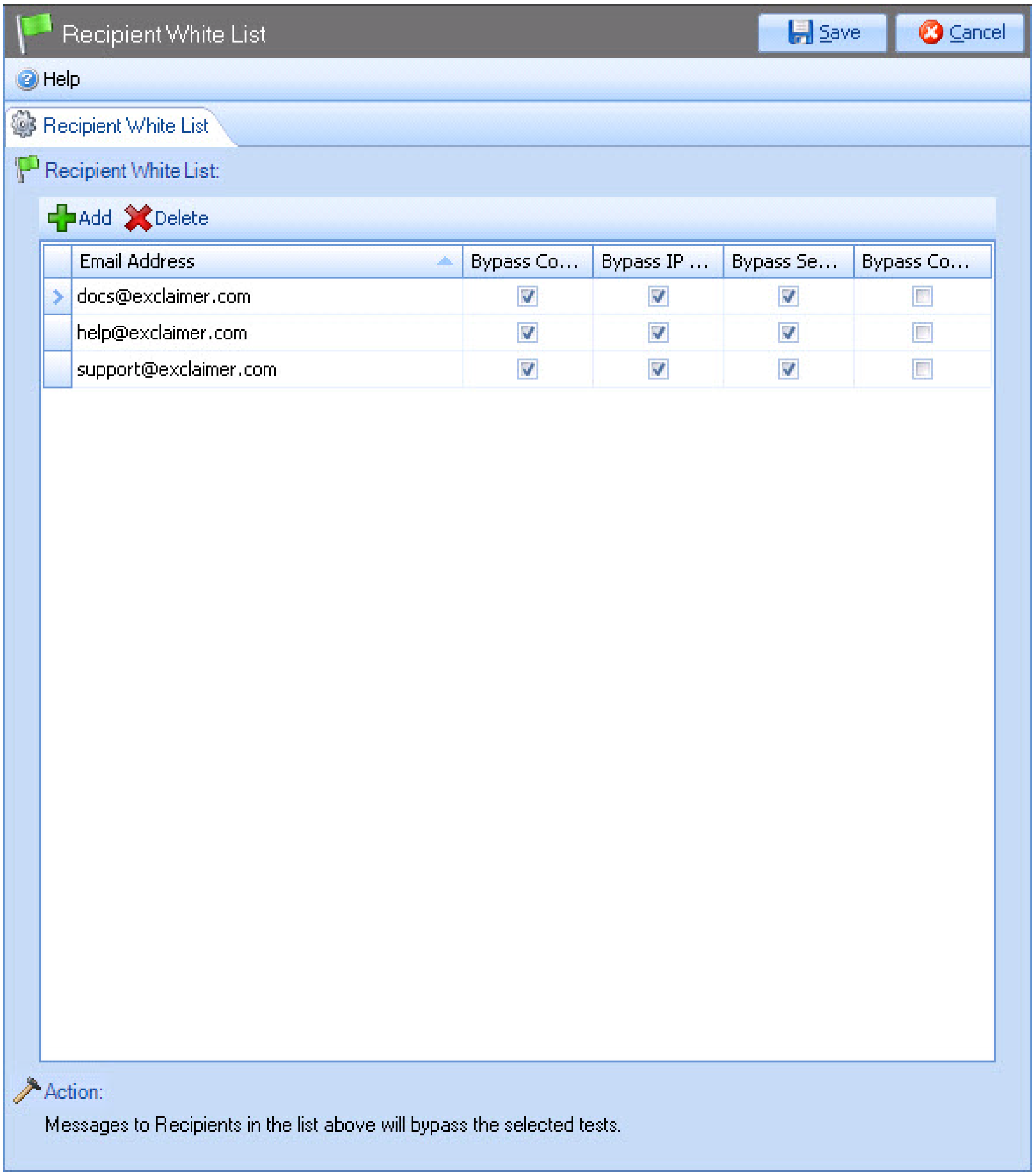
- Understanding the recipient white list window [pg.85]
- Adding recipients to the recipient white list [pg.86]
- Updating recipient white list settings for an existing entry [pg.87]
- Deleting recipients from the recipient white list [pg.88]

The **recipient white list** rule will only be applied if the recipient filtering feature [pg.161] is enabled.

Understanding the Recipient White List Window

The recipient white list window displays email addresses which are exempt from some or all anti-spam checks for any email messages received. Each entry is associated with an email address and required white list settings. From here you can add a new entry [pg.86], update settings for an existing entry [pg.87] or you can delete an existing entry [pg.88].

For each entry in the recipient white list, you can choose to enforce or bypass any of the available anti-spam rules, as shown below:



Email Address	Bypass Co...	Bypass IP ...	Bypass Se...	Bypass Co...
docs@exclaimer.com	☑	☑	☑	□
help@exclaimer.com	☑	☑	☑	□
support@exclaimer.com	☑	☑	☑	□

Messages to Recipients in the list above will bypass the selected tests.

Any of the Exclaimer Anti-spam rules can be checked or unchecked as required. If an option is checked (ticked) it means that the rule will **not** be applied to any messages which have been sent to this address.

Default Settings

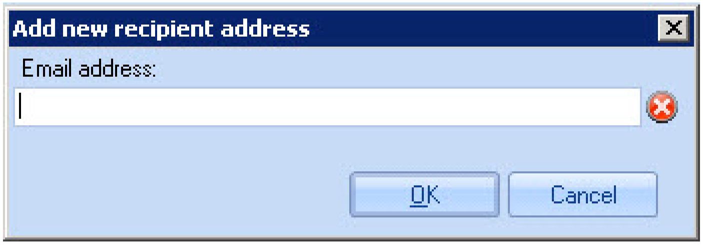
When an email address is added to the recipient white list, default settings are that all anti-spam rules are checked (i.e. set to be ignored) except for Commtouch classifications.

The default is set in this way because Commtouch [pg.106] checks are considered to be so accurate that it is worth applying this rule under any circumstances. However, this is only a recommended setting and default options can be changed as required.

Adding Recipients to the Recipient White List

To add an address to the recipient white list, follow the steps below:

1. Expand the Anti-spam rules branch of the Exclaimer console tree [pg.34].
2. Select the recipient white list branch to display the recipient white list window.
3. Click the add button to open the add new recipient address window:



4. Type the full address (e.g. joe.bloggs@exclaimer.com) into the email address field.

> You do not need to worry about adding duplicate entries to the **recipient white list**. When an email address is added the system checks to see if it already exists and, if the address is found, it is not added again.

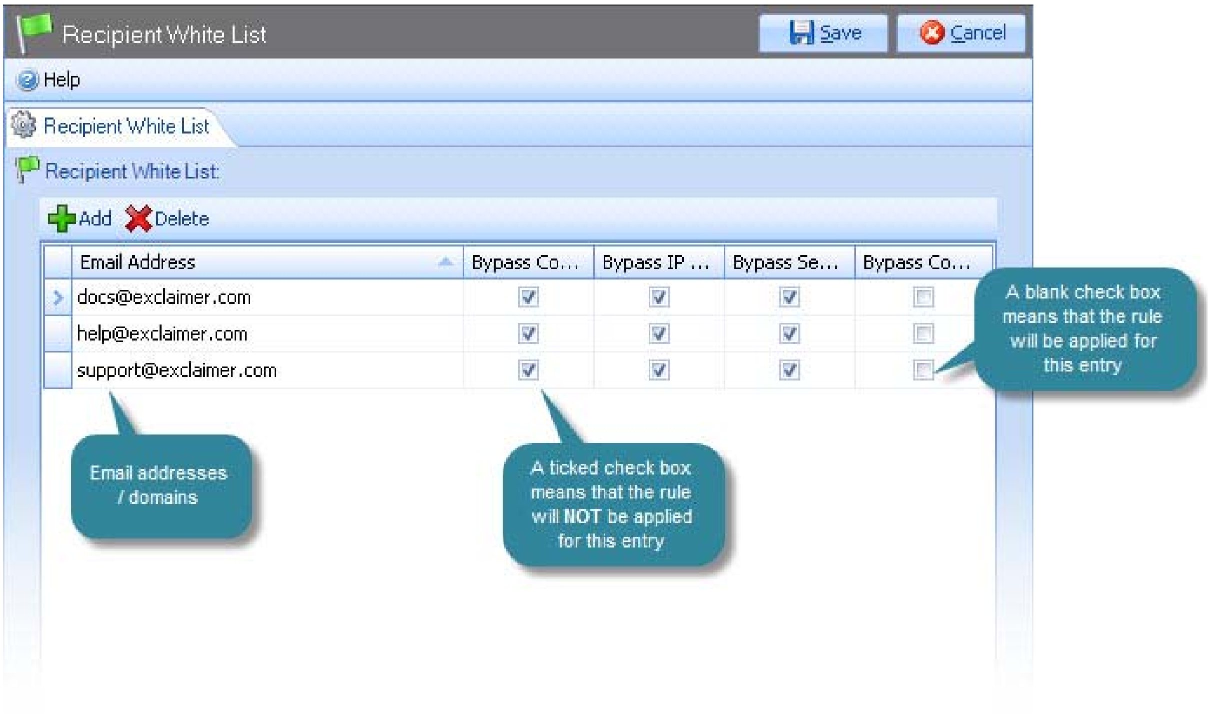
5. Click OK to add the address to the list exit back to the recipient white list window.

> When an email address is added to the **recipient white list**, default settings are that all **Anti-spam** rules are checked (i.e. set to be ignored) except for **Commtouch classification**. The default is set in this way because **Commtouch** checks are considered to be so accurate that it is worth applying this rule under any circumstances. However, this is only a recommended setting and default options can be changed as required.

6. Add further addresses as required.
7. Click the save button (at the top of the window) to save changes.

Updating Recipient White List Settings for an Existing Entry

Each entry in the recipient white list is associated with an email address and a series of check boxes that determine which rules (i.e. anti spam checks) are applied for the entry and which rules should not be applied:



Email Address	Bypass Co...	Bypass IP ...	Bypass Se...	Bypass Co...
docs@exclaimer.com	☑	☑	☑	□
help@exclaimer.com	☑	☑	☑	□
support@exclaimer.com	☑	☑	☑	□

A blank check box means that the rule will be applied for this entry

Email addresses / domains

A ticked check box means that the rule will NOT be applied for this entry

Here, a ticked check box means that the rule will **not** be applied for the associated email address and conversely, a blank check box means that the rule will be applied. If you wish to change these settings for an email address, simply select and de-select associated check boxes as required.

> If an email address has been entered incorrectly (or has been changed) you should delete the entry [pg.88] from the **recipient white list** and add a new entry [pg.86] for the required address.

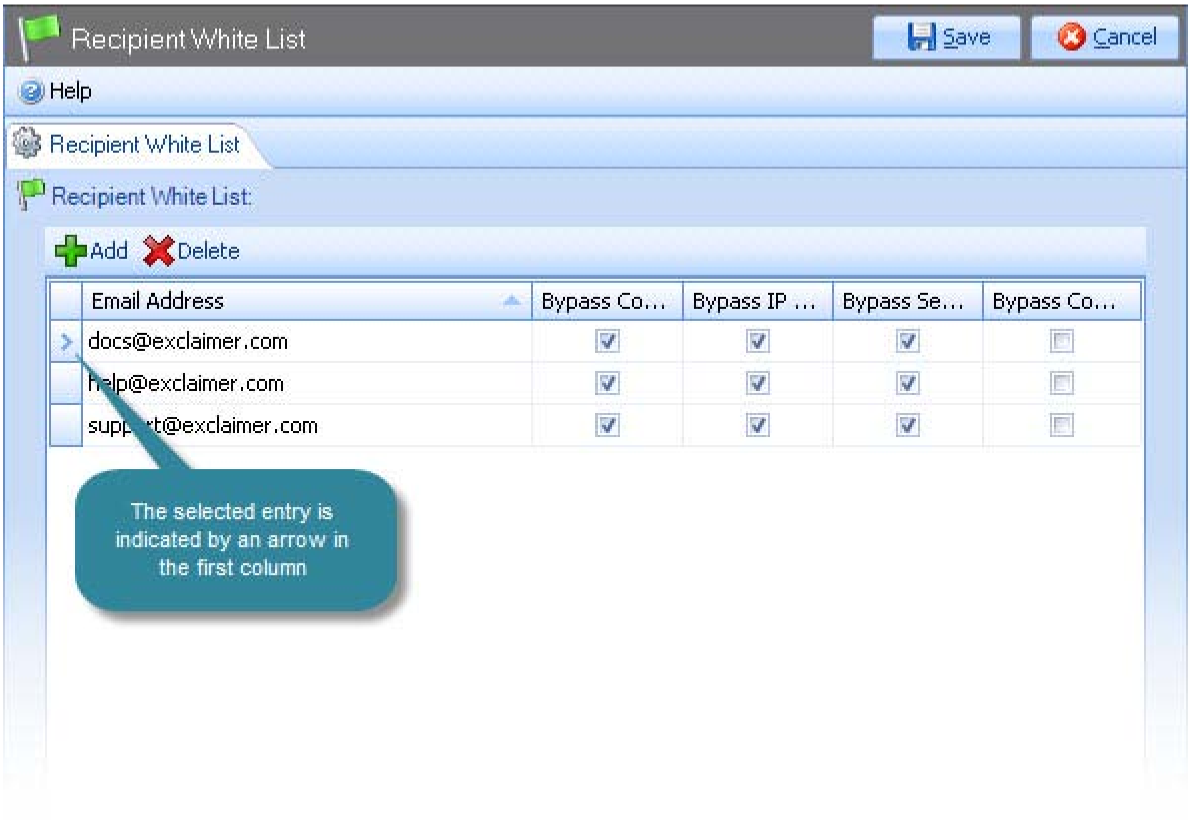
Deleting Recipients from the Recipient White List

To remove an address from the recipient white list, follow the steps below:

1. Expand the Anti-spam rules branch of the Exclaimer console tree [pg.34].

2. Select the recipient white list branch to display the recipient white list window.

3. Select the entry that you wish to delete:



	Email Address	Bypass Co...	Bypass IP ...	Bypass Se...	Bypass Co...
>	docs@exclaimer.com	☑	☑	☑	☐
	help@exclaimer.com	☑	☑	☑	☐
	support@exclaimer.com	☑	☑	☑	☐

The selected entry is indicated by an arrow in the first column

4. Click the delete button. You are asked if you are sure that the selected entry should be removed.

5. If you are satisfied that the correct entry has been selected, click yes to remove the entry and exit back to the recipient white list window.

6. Click the save button (at the top of the window) to save changes.

Sender ID

Sender ID filtering is used to help counter email spoofing. Email spoofing is a deceptive practice that is commonly adopted by spammers; it involves altering email headers so that messages appear to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to make recipients open (and possibly even respond to) their solicitations.

Sender ID works by verifying that every email message does actually originate from the Internet domain from which it was sent. This is achieved using an email validation system - the Sender Policy Framework (SPF). Sender Policy Framework (SPF) is an email validation system which was designed to prevent spam. It allows the owner of an Internet domain to specify which machines are authorized to send email for that domain by creating a specific SPF record in the public Domain Name System (DNS). The DNS is then used to check that email from a given domain is being sent by a host that has been sanctioned by the owner of that domain.

When Sender ID filtering takes place, an SPF result is assigned to messages. There are a range of possible results, including:

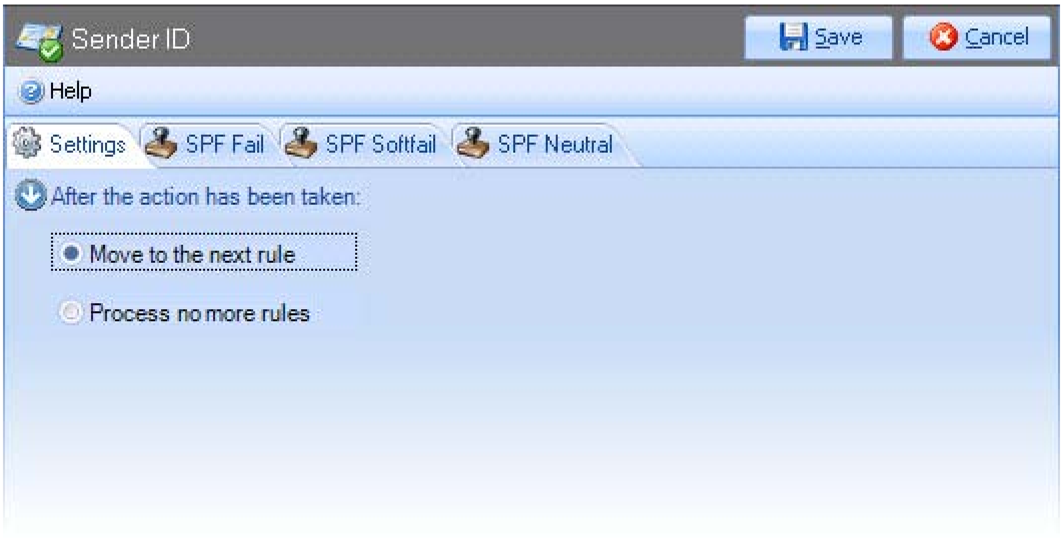
SPF Result	Summary
None	This result is given when no SPF records are published for the domain.
Neutral	This result is given when the domain owner has explicitly stated that they cannot or do not want to assert whether or not the sending IP address is authorized.
Pass	This result is given when the SPF record designates the sending IP address to be allowed to send email.
Fail	This result is given when the SPF record does not designate the sending IP address to send emails for the particular domain.
SoftFail	This result should be treated as somewhere between fail and neutral. It is given when the SPF record does not explicitly designate the sending IP address to send emails for the particular domain.

Within Exclaimer Anti-spam, you can define what actions should be taken with messages which are given an SPF result of neutral [pg.97], fail [pg.91] or softfail [pg.94] as a result of Sender ID filtering. You can also use general Sender ID settings [pg.90] to determine whether Exclaimer Anti-spam should continue processing rules once Sender ID filtering is complete, or to stop processing rules at this point.

The **sender ID** rule will only be applied if the sender ID feature [pg.166] is enabled.

Sender ID Settings

Sender ID settings are used to determine whether or not Exclaimer Anti-spam should continue processing rules once Sender ID filtering is complete, or whether to stop:



After the action has been taken:

● Move to the next rule

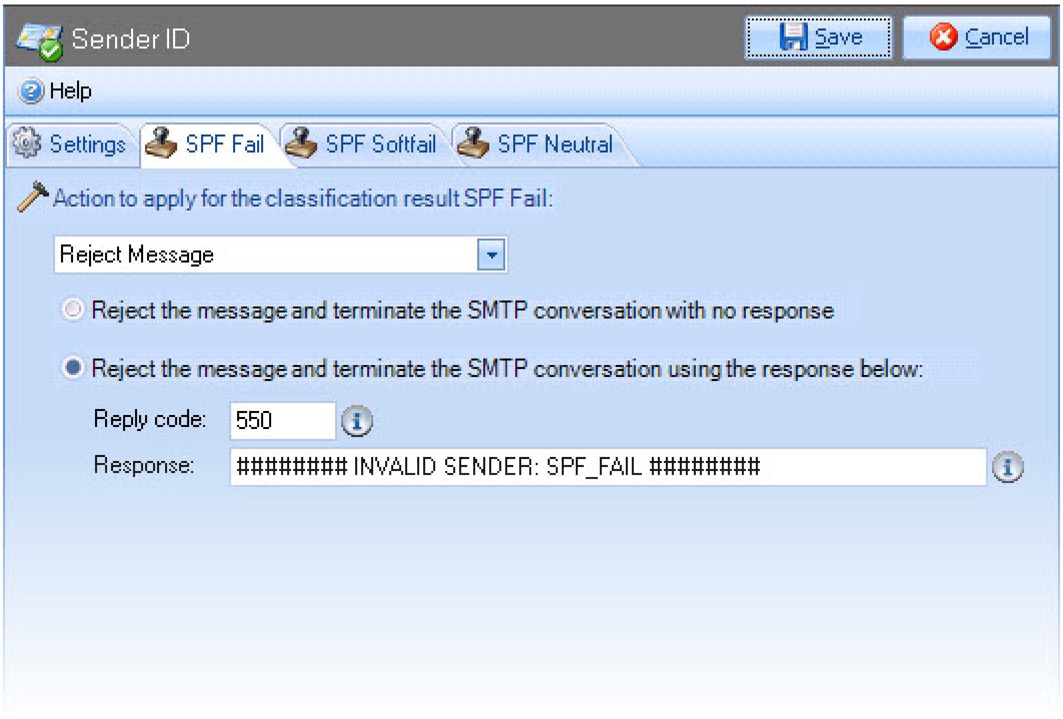
○ Process no more rules

These options are summarized below:

Option	Summary
Move to next rule	Rules are processed in the same sequence that they appear in the console tree - namely: • Sender block list [pg.67] • Sender white list [pg.77] • Recipient white list [pg.84] • Sender ID [pg.89] • Content filtering [pg.100] • Commtouch classifications [pg.106] Select this option if you wish to continue processing rules (i.e. continue to Commtouch [pg.106] checks) when Sender ID filtering is complete.
Process no more rules	If you wish to stop processing rules when Sender ID filtering is complete, select this option.

SPF Fail Settings

The SPF fail tab is used to define what action should be taken if Sender ID filtering returns an SPF result of fail [pg.89]:



Action to apply for the classification result SPF Fail:

Reject Message

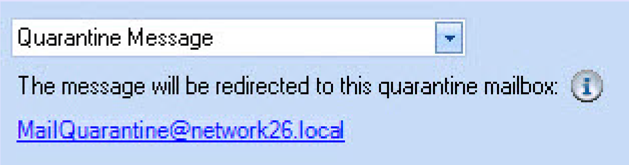
○ Reject the message and terminate the SMTP conversation with no response

● Reject the message and terminate the SMTP conversation using the response below:

Reply code: 550

Response: ######### INVALID SENDER: SPF_FAIL #########

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.

.../continued

Option	Summary
Reject message	Select this option to reject the message, then set additional options as follows: • Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. • Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code: SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Response: Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: • Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. • Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value. • Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content).

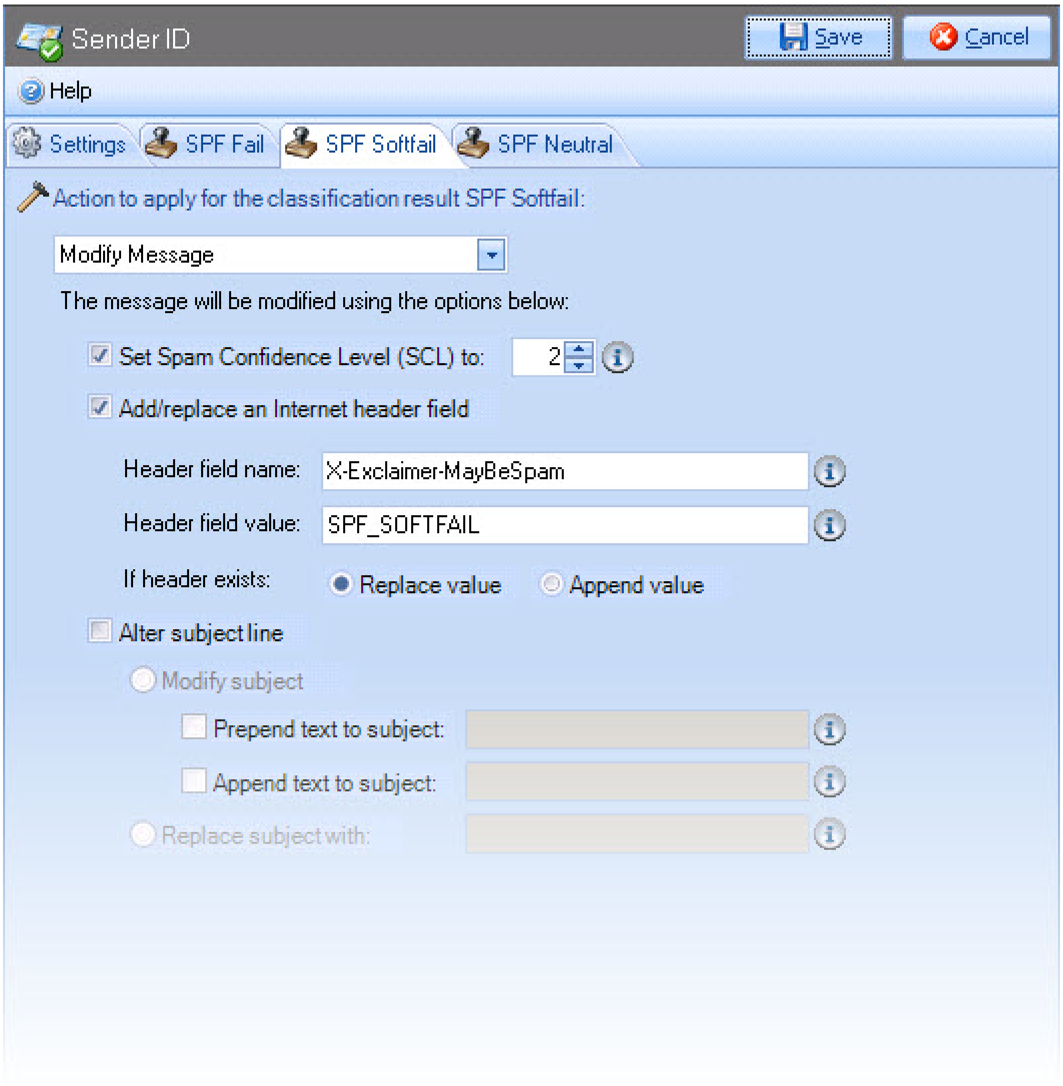
.../continued

<table>
<tr><th>Option</th><th>Summary</th></tr>
<tr><td></td><td>Subject line options can be set as follows:
<table>
<tr><td>Modify subject...</td><td>Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message.
Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message.</td></tr>
<tr><td>Replace subject with...</td><td>Select this option and specify text to be used instead of the original subject line of the email message.</td></tr>
</table>
If required you can choose to modify a combination of <b>SCL</b>, <b>Internet header</b> and <b>subject line</b> options.</td></tr>
</table>

The recommended setting for an **SPF result** of **fail** is to reject messages and terminate the SMTP conversation with a reply code of **550**.

SPF Softfail Settings

The SPF softfail tab is used to define what action should be taken if Sender ID filtering returns an SPF result of softfail [pg.89]:



Action to apply for the classification result SPF Softfail:

Modify Message

The message will be modified using the options below:

☑ Set Spam Confidence Level (SCL) to: 2

☑ Add/replace an Internet header field

Header field name: X-Exclaimer-MayBeSpam

Header field value: SPF_SOFTFAIL

If header exists: ● Replace value ○ Append value

□ Alter subject line

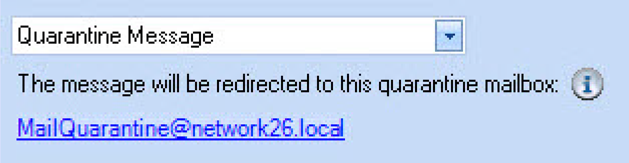
○ Modify subject

□ Prepend text to subject:

□ Append text to subject:

○ Replace subject with:

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.
Reject message	Select this option to reject the message, then set additional options as follows: • Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. • Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code: SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response: Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.

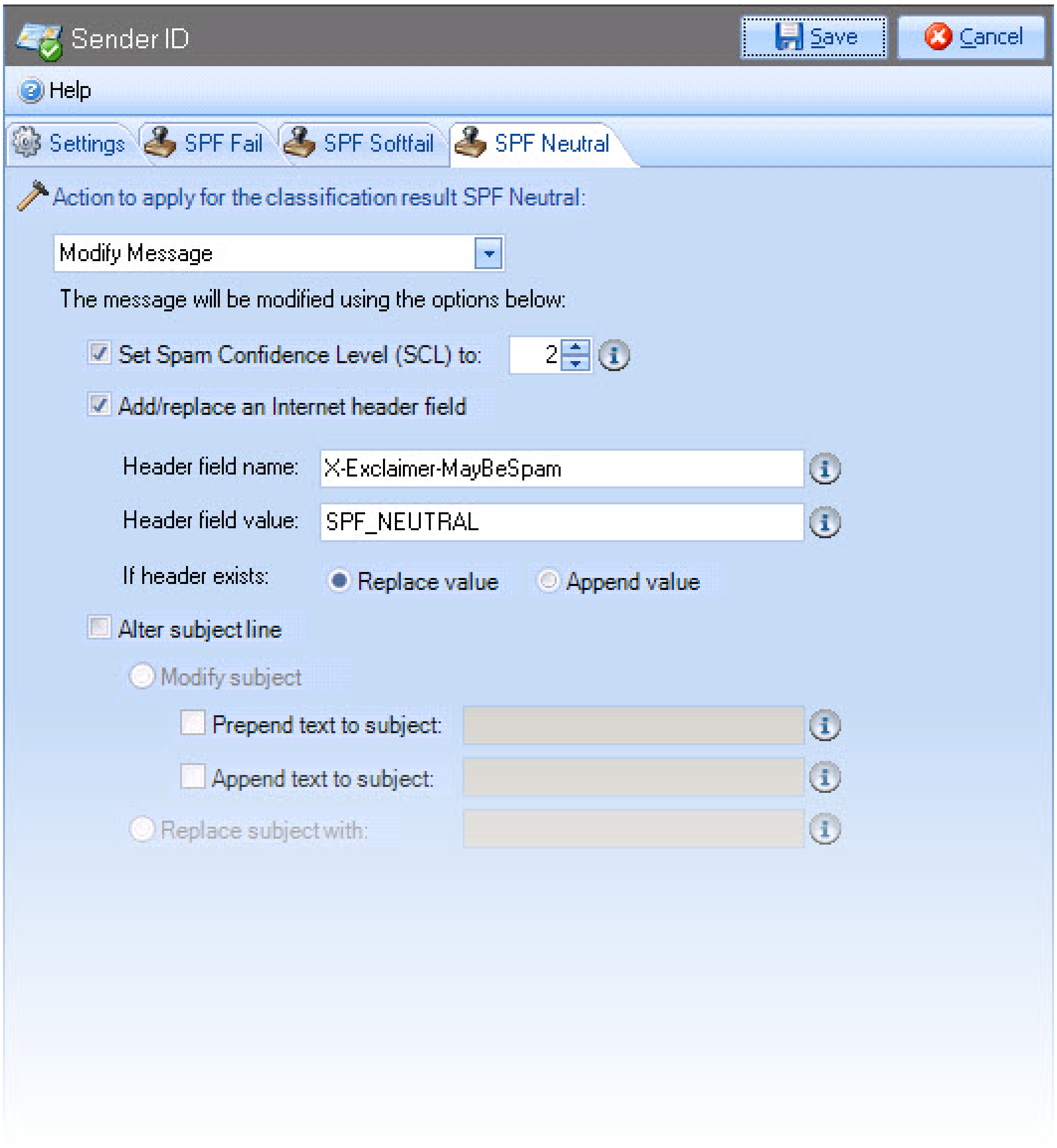
.../continued

<table>
<thead>
<tr><th>Option</th><th>Summary</th></tr>
</thead>
<tbody>
<tr>
<td>Modify message</td>
<td>Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows:
- Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100].
- Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value.
- Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows:
<table>
<tr><td>Modify subject...</td><td>Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message.
Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message.</td></tr>
<tr><td>Replace subject with...</td><td>Select this option and specify text to be used instead of the original subject line of the email message.</td></tr>
</table>
If required you can choose to modify a combination of <b>SCL</b>, <b>Internet header</b> and <b>subject line</b> options.</td>
</tr>
</tbody>
</table>

The recommended setting for an **SPF result** of **softfail** is to modify messages by setting the **SCL** rating to **2** and replacing any existing value for the **X-Exclaimer-MayBeSpam** header field with **SPF_SOFTFAIL**.

SPF Neutral Settings

The SPF neutral tab is used to define what action should be taken if Sender ID filtering returns an SPF result of neutral [pg.89]:



Action to apply for the classification result SPF Neutral:

Modify Message

The message will be modified using the options below:

☑ Set Spam Confidence Level (SCL) to: 2

☑ Add/replace an Internet header field

Header field name: X-Exclaimer-MayBeSpam

Header field value: SPF_NEUTRAL

If header exists: ● Replace value ○ Append value

□ Alter subject line

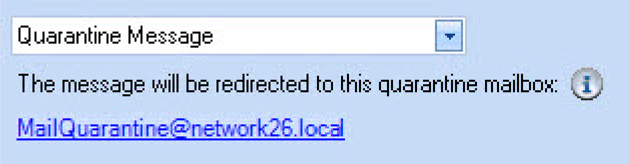
○ Modify subject

□ Prepend text to subject:

□ Append text to subject:

○ Replace subject with:

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.
Reject message	Select this option to reject the message, then set additional options as follows: • Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. • Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code: SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response: Whilst the reply code uses a standard number and text, the response field allows you to enter additional text to be inserted in the rejection message.

.../continued

Option	Summary
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: • Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. • Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value. • Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows: Modify subject... — Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message. Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message. Replace subject with... — Select this option and specify text to be used instead of the original subject line of the email message. If required you can choose to modify a combination of **SCL**, **Internet header** and **subject line** options.

The recommended setting for an **SPF result** of **neutral** is to modify messages by setting the **SCL** rating to **2** and replacing any existing value for the **X-Exclaimer-MayBeSpam** header field with **SPF_NEUTRAL**.

Content Filtering

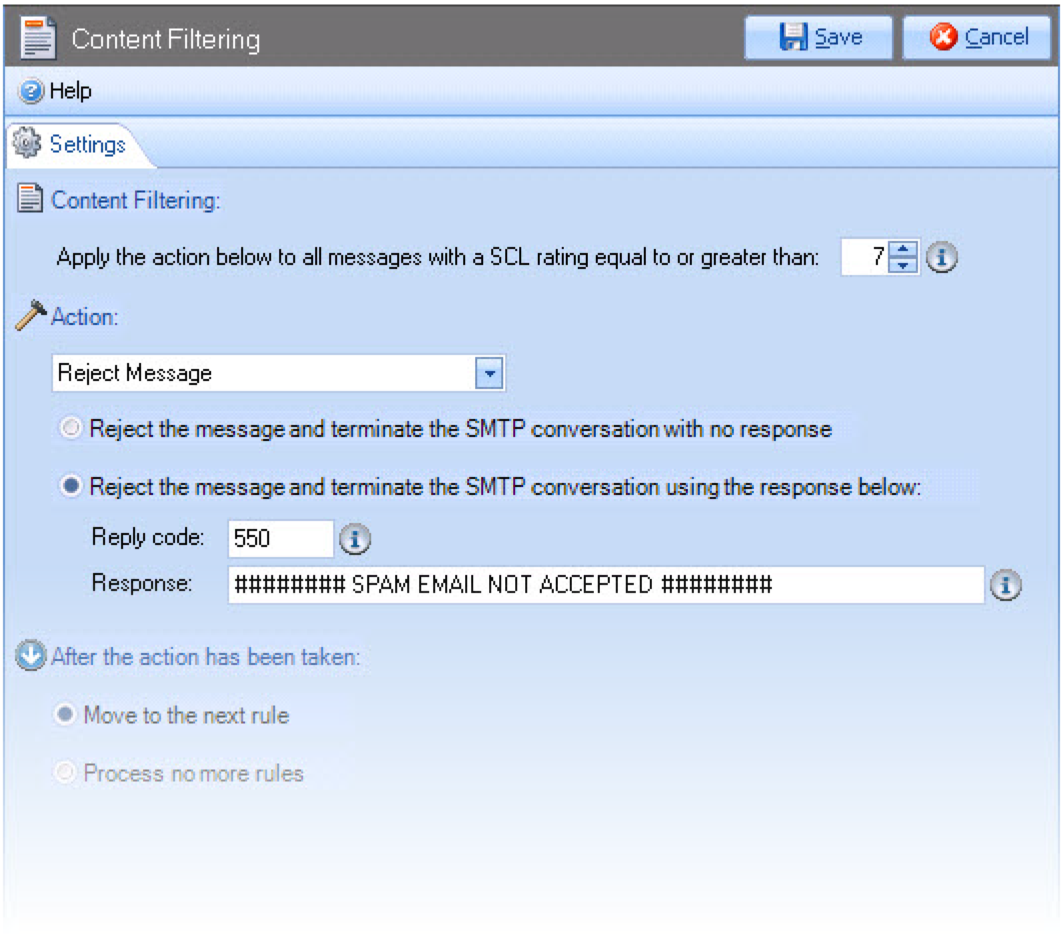
When email messages are received, textual content is evaluated and a Spam Confidence Level (SCL) rating is assigned and stored as an attribute of the message. The SCL rating is applied by the Microsoft Exchange Content Filtering Agent, using Microsoft SmartScreen® Filter technology.

An SCL rating is a number between 0 and 9 where 0 indicates that the message is highly unlikely to be spam and a rating of 9 indicates that the message is very likely to be spam. Using content filtering options [pg.101] within Exclaimer Anti-spam, you can define an SCL threshold which, when reached, will trigger required actions. The nature of these actions can also be defined using Exclaimer Anti Spam's content filtering options [pg.101].

You can build a list of custom words which should be allowed or blocked using the custom words tab [pg.173] (located within the content filtering feature [pg.170]). If you find that certain words are not being identified as spam when they should be, you can add them to a **block list** and conversely, if you find that certain words are causing messages to be identified as spam erroneously, you can add them to an **allow** list. Also note that the **content filtering** rule will only be applied if the **content filtering feature** is enabled.

Content Filtering Options

All content filtering options are available from a settings tab when the content filtering branch is selected in the Exclaimer console tree [pg.34]:



Content Filtering:

Apply the action below to all messages with a SCL rating equal to or greater than: 7

Action:

Reject Message

○ Reject the message and terminate the SMTP conversation with no response

● Reject the message and terminate the SMTP conversation using the response below:

Reply code: 550

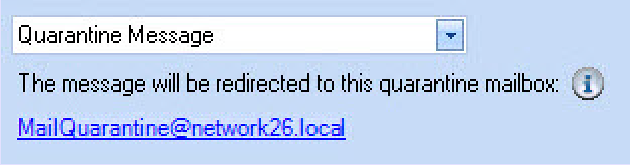
Response: ######## SPAM EMAIL NOT ACCEPTED ########

After the action has been taken:

● Move to the next rule

○ Process no more rules

These options are summarized below:

Option	Summary
Content filtering	
Apply the action below to all messages with a SCL rating equal to or greater than...	Select an SCL rating which, when reached or surpassed, will trigger actions defined in subsequent sections of this settings tab. For example, you may wish to simply reject any messages with an SCL rating greater than or equal to 7, or you might take a 'softer' approach and choose to modify messages with an SCL rating greater than or equal to 4 on the basis that subsequent sender ID [pg.89] and Commtouch [pg.106] rules will confirm whether the messages are really spam.
Action	
Use the drop-down list to select the required action to be taken with messages that reach the specified SCL rating. Subsequent options may be displayed, dependent upon which entry is selected from this list.	
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.

.../continued

<table>
<tr><th>Option</th><th>Summary</th></tr>
<tr><td>Reject message</td><td>Select this option to reject the message, then set additional options as follows:
Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future.
● Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message:
<table>
<tr><td>Reply code</td><td>SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server.
These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: <i>Requested actions not taken - mailbox unavailable</i>.
Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used).</td></tr>
<tr><td>Response</td><td>Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.</td></tr>
</table>
</td></tr>
</table>

.../continued

Option	Summary
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: • Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value. • Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows: Modify subject... — Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message. Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message. Replace subject with... — Select this option and specify text to be used instead of the original subject line of the email message. If required you can choose to modify a combination of SCL, Internet header and subject line options. .../continued

Option	Summary
After the action has been taken...	
Move to next rule	Rules are processed in the same sequence that they appear in the console tree - namely: - Recipient white list [pg.84] - Sender white list [pg.77] - Sender block list [pg.67] - Content filtering [pg.100] - Sender ID [pg.89] - Commtouch classifications [pg.106] Select this option if you wish to continue processing rules (i.e. continue to sender ID [pg.89] checks) after specified actions have been applied to email messages.
Process no more rules	If you wish to stop processing rules after specified actions have been applied to email messages, select this option. If you have chosen to reject messages [pg.103] which are greater than or equal to a given SCL rating, it is logical to select the **process no more rules** option. However, if you have chosen another action, it is more likely (though not mandatory) that you will want to **move to the next rule**.

You can build a list of custom words which should be allowed or blocked using the custom words tab [pg.173] (located within the **content filtering feature**). If you find that certain words are not being identified as spam when they should be, you can add them to a **block list** and conversely, if you find that certain words are causing messages to be identified as spam erroneously, you can add them to an **allow** list.

Commtouch Classifications

Exclaimer Anti-spam has integrated the Commtouch anti-spam solution to offer an additional layer of security. This solution is based upon the most fundamental characteristic of all spam and malware - mass distribution. Rather than evaluating individual messages, Commtouch uses its own Recurrent Pattern Detection™ (RPD™) technology which focuses on detecting patterns in large scale spam attacks.

RPD™ probes the Internet to gather and analyze information about spam outbreak. On average, RPD™ technology recognizes unique recurrent patterns in new spam attacks within the first 1.5 minutes of an outbreak. Since it does not rely on the content of email messages, RPD™ can detect spam in any language and in every message format (including images, HTML and non-English characters).

New spam and malware outbreaks are identified as soon as they emerge, and recorded in the Commtouch Detection Center. The Commtouch Anti-Spam Detection Center holds a vast database of already classified patterns with new classifications being added every day. Having integrated the Commtouch solution, Exclaimer Anti-spam can interrogate this database and obtain classifications for incoming email messages in real time.

Within Exclaimer Anti-spam, you can specify what action should be taken with email messages which are given the following Commtouch classifications:

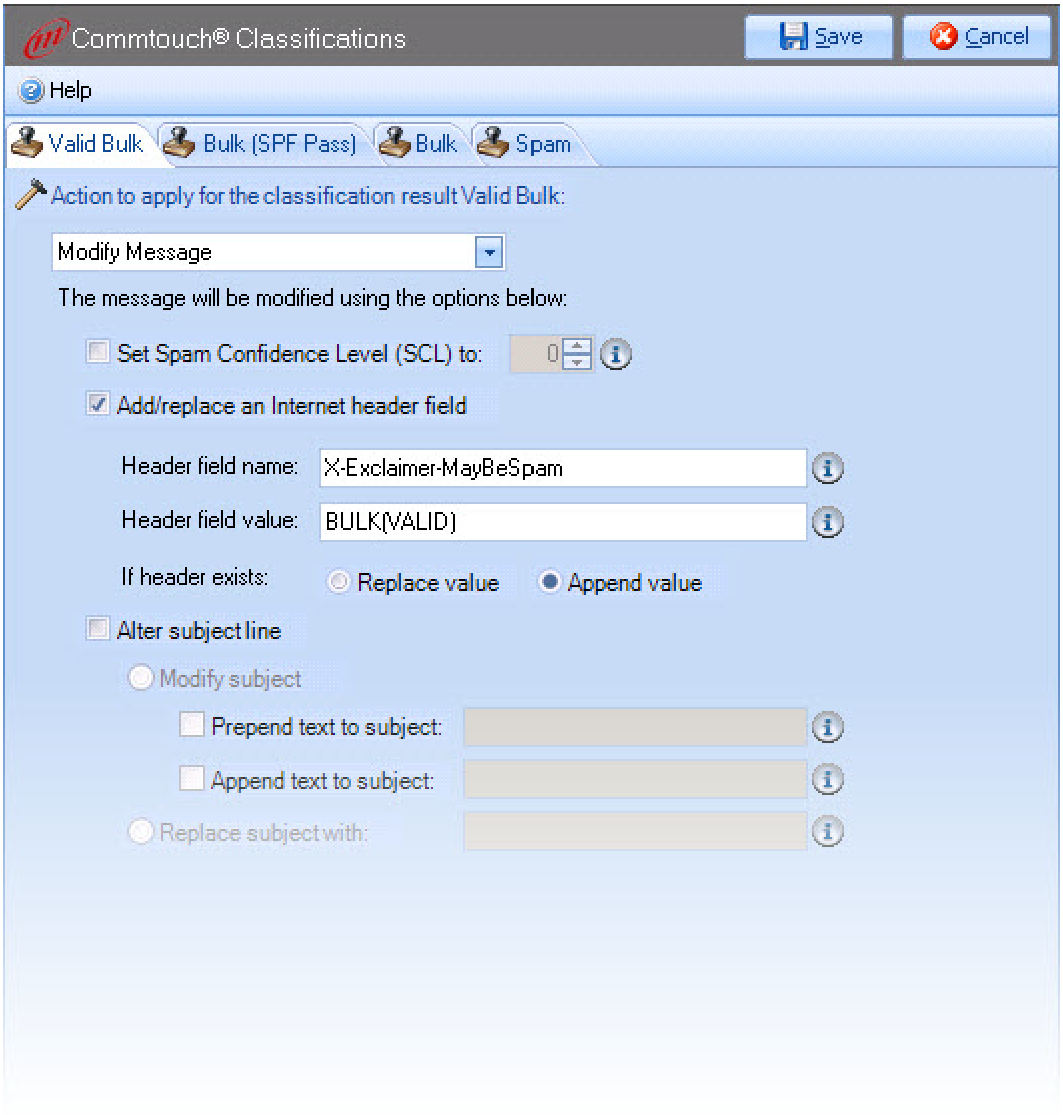
Commtouch classification	Summary
Valid bulk	Websites that send bulk emails and have registered with Commtouch. Emails from these sites are received by subscription only and typically contain marketing material. Such messages will always have a clear unsubscribe link.
Bulk (SPF pass)	Websites that are not registered with Commtouch but which Commtouch have identified as sending bulk email campaigns. The email is from an email domain that has a valid SPF record [pg.89] which goes some way to ensure that the sender is legitimate and therefore that the message is less likely to be spam.
Bulk	Websites that are not registered with Commtouch but which Commtouch have identified as sending bulk email campaigns. The email is from an email domain that does not have a valid SPF record [pg.89] which means that the message is more likely to be spam, though Commtouch has not categorised them as a known spammer.
Spam	Websites that, based upon past monitoring of global email, Commtouch has identified as being a known source of spam.

The **Commtouch classifications** rule will only be applied if the Commtouch feature [pg.191] is enabled.

Valid Bulk Settings

If a message is classified as valid bulk it means that the message originates from a sender of bulk emails which is registered with Commtouch. These emails are sent on a subscription-only basis and typically contain marketing material. Such messages will always have a clear unsubscribe link.

The valid bulk tab is used to define what action should be taken if Commtouch returns a classification of valid bulk:



Action to apply for the classification result Valid Bulk:

Modify Message

The message will be modified using the options below:

□ Set Spam Confidence Level (SCL) to: 0

☑ Add/replace an Internet header field

Header field name: X-Exclaimer-MayBeSpam

Header field value: BULK(VALID)

If header exists: ○ Replace value ● Append value

□ Alter subject line

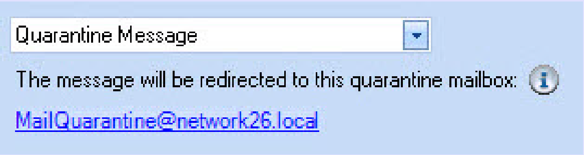
○ Modify subject

□ Prepend text to subject:

□ Append text to subject:

○ Replace subject with:

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.
Reject message	Select this option to reject the message, then set options as follows: • Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. • Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code: SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response: Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.

.../continued

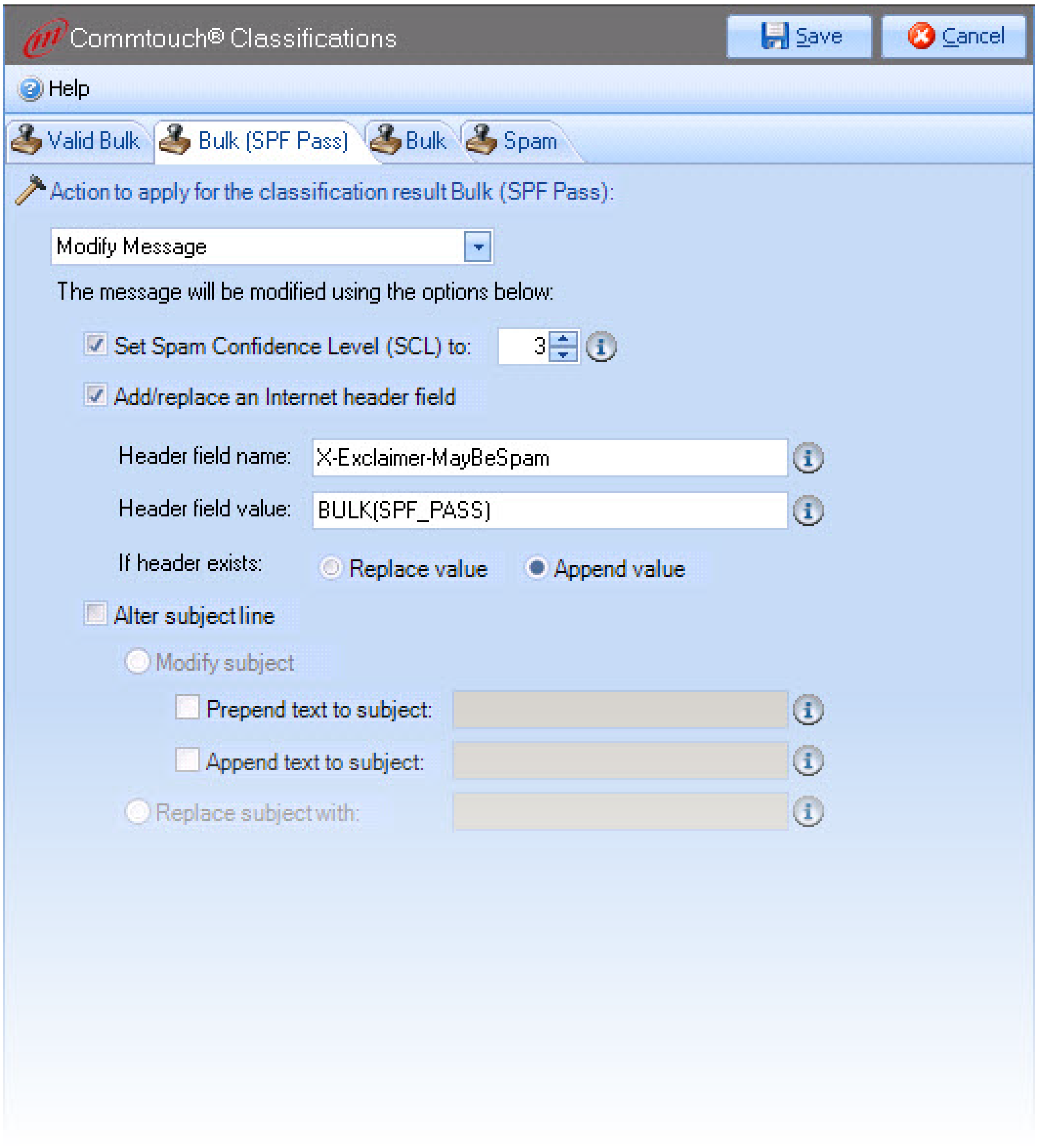
<table>
<tr><th>Option</th><th>Summary</th></tr>
<tr><td>Modify message</td><td>Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows:
- Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100].
Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value.
- Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows:
<table>
<tr><td>Modify subject...</td><td>Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message.
Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message.</td></tr>
<tr><td>Replace subject with...</td><td>Select this option and specify text to be used instead of the original subject line of the email message.</td></tr>
</table>
If required you can choose to modify a combination of <b>SCL</b>, <b>Internet header</b> and <b>subject line</b> options.</td></tr>
</table>

The recommended setting for a **Commtouch** classification of **valid bulk** is to deliver the message normally, without any modifications.

Bulk (SPF Pass) Settings

If a message is classified as bulk (SPF pass) it means that the message originates from a sender that is not registered with Commtouch but which Commtouch have identified as sending bulk email campaigns. The email is from an email domain that does have a valid SPF record [pg.89] which goes some way to ensure that the sender is legitimate and therefore that the message is less likely to be spam.

The bulk (SPF pass) tab is used to define what action should be taken if Commtouch returns a classification of bulk (SPF pass):



Action to apply for the classification result Bulk (SPF Pass):

Modify Message

The message will be modified using the options below:

☑ Set Spam Confidence Level (SCL) to: 3

☑ Add/replace an Internet header field

Header field name: X-Exclaimer-MayBeSpam

Header field value: BULK(SPF_PASS)

If header exists: ○ Replace value ● Append value

☐ Alter subject line

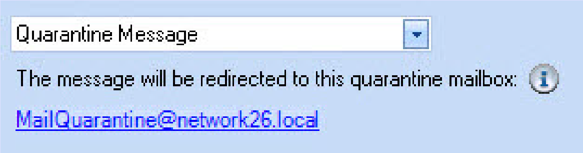
○ Modify subject

☐ Prepend text to subject:

☐ Append text to subject:

○ Replace subject with:

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.
Reject message	Select this option to reject the message, then set options as follows: • Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. • Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code: SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response: Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.

.../continued

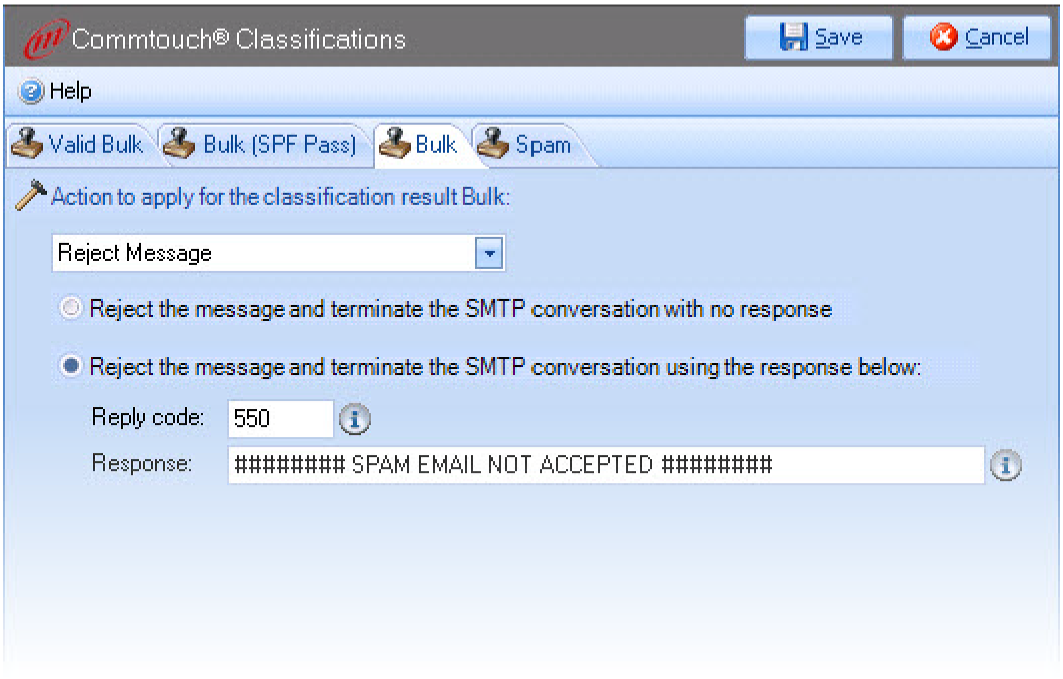
Option	Summary
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: ● Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. ● Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value. ● Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows: Modify subject... — Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message. Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message. Replace subject with... — Select this option and specify text to be used instead of th original subject line of the email message. If required you can choose to modify a combination of **SCL**, **Internet header** and **subject line** options.

The recommended setting for a **Commtouch** classification of **bulk (SPF pass)** is to modify messages by replacing any existing value for the **X-Exclaimer-MayBeSpam** header field with **BULK(SPF_PASS)**.

Bulk Settings

If a message is classified as bulk it means that the message originates from a sender that is not registered with Commtouch but which Commtouch have identified as sending bulk email campaigns. The email is from an email domain that does not have a valid SPF record [pg.89] which means that the message is more likely to be spam, though Commtouch has not categorised them as a known spammer.

The bulk tab is used to define what action should be taken if Commtouch returns a classification of bulk:



Action to apply for the classification result Bulk:

Reject Message

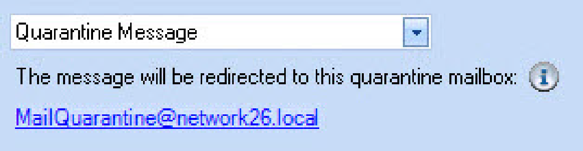
○ Reject the message and terminate the SMTP conversation with no response

● Reject the message and terminate the SMTP conversation using the response below:

Reply code: 550

Response: ######## SPAM EMAIL NOT ACCEPTED ########

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.
Reject message	Select this option to reject the message, then set options as follows: - Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. - Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code: SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response: Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.

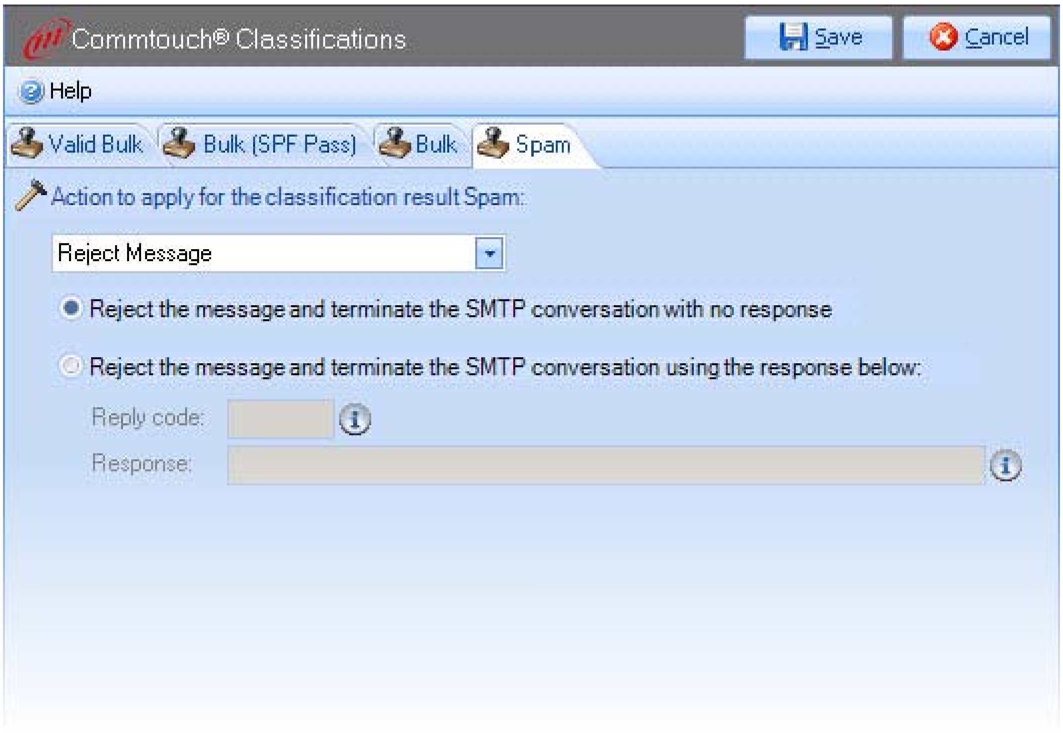
.../continued

Option	Summary
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: ● Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. ● Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value. ● Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows: Modify subject... — Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message. Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message. Replace subject with... — Select this option and specify text to be used instead of the original subject line of the email message. If required you can choose to modify a combination of **SCL**, **Internet header** and **subject line** options.

The recommended setting for a **Commtouch** classification of **bulk** is to reject the message with a reply code of **550**.

Spam Settings

If a message is classified as spam it means that the message originates from a sender that, based upon past monitoring of global email, Commtouch has identified as being a known source of spam. The spam tab is used to define what action should be taken if Commtouch returns a classification of spam:



Action to apply for the classification result Spam:

Reject Message

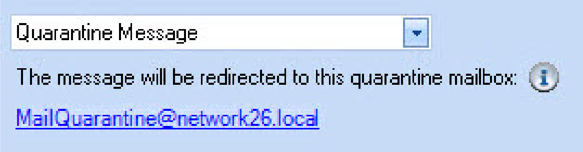
● Reject the message and terminate the SMTP conversation with no response

○ Reject the message and terminate the SMTP conversation using the response below:

Reply code:

Response:

These options are summarized below:

Option	Summary
Deliver message	Select this option to simply deliver the message as normal, without any modifications.
Deliver message to junk e-mail folder	Select this option to deliver email messages to the recipient's Junk e-mail folder. No additional settings are prompted when this option is selected.
Quarantine message	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58]. If you have defined a Quarantine Mailbox, it will be displayed when the quarantine message options is selected here - for example:  Quarantine Message The message will be redirected to this quarantine mailbox: MailQuarantine@network26.local A hyperlink is displayed so you can access Exclaimer Anti-spam options [pg.58] and set/change the required mailbox.

.../continued

Option	Summary
Reject message	Select this option to reject the message, then set options as follows: - Reject the message and terminate the SMTP conversation with no response. Choose this option if you simply want to reject the message (i.e. ensure that it is not delivered to recipients) without any form of response to the sender. This is the accepted way of dealing with spam senders because, if they do not receive a reply, they assume that there is no email server and so are less likely to target your server in future. - Reject the message and terminate the SMTP conversation using the response below. Choose this option to send a return email which can include a reply code and a response message: Reply code SMTP reply codes are a standard set of codes which are used to ensure that mail transfer requests and actions are always in step, and to ensure that the SMTP client always knows the state of the SMTP server. These codes are comprised of a three-digit number, followed by some text. The default setting is number 550 which is associated with the following text: *Requested actions not taken - mailbox unavailable*. Reply code number 550 is specified by default. This is the recommended setting but you can use an alternative code if required (any standard SMTP response code can be used). Response Whilst the reply code uses a standard number and text, the response field allows you to enter some additional text to be inserted in the rejection message.
Modify message	Select this option to modify the message. These modifications might be used to determine whether or not the message is delivered to recipients, as follows: - Set spam confidence level (SCL) to. Choose this option if you wish to change the SCL to a value between 0 and 9. For further information about SCL ratings see content filtering [pg.100]. - Add/replace an Internet header field. Every message has headers which are structured into fields, where each field has a name and a value. These fields can be used as criteria for an Outlook rule (for example, users might define an Outlook rule to move messages with a given header value to a specified folder) or they might be used by other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by an Internet header value). To change an Internet header field, specify the header field name, the required header field value, then choose whether this value should replace any existing value or the field, or append any existing value.

.../continued

Option	Summary
	● Alter subject line. Choose this option if you wish to modify the subject line of email messages. This might be useful (for example) if users have defined Outlook rules to handle messages with a given subject line, or if you use other Exclaimer products (for example Exclaimer Auto Responder might contain policies which are triggered by subject line content). Subject line options can be set as follows: Modify subject... — Prepend text to subject. Select this option and specify text to be inserted in front of the original subject line of the email message. Append text to subject. Select this option and specify text to be inserted at the end of the original subject line of the email message. Replace subject with... — Select this option and specify text to be used instead of the original subject line of the email message. If required you can choose to modify a combination of **SCL**, **Internet header** and **subject line** options.

The recommended setting for a **Commtouch** classification of **spam** is to reject the message with a reply code of **550**.

Chapter 6

Exclaimer Anti-spam: Features

Introduction

Within Exclaimer Anti-spam, features are used to define core configuration for Microsoft Exchange anti-spam filters, together with additional Exclaimer Anti-spam options.

Having installed Exclaimer Anti-spam, its features are pre-configured and it is unlikely that you will need to update features on more than an occasional basis. If you do need to change these settings, it is likely that you will require at least a basic knowledge of Microsoft Exchange anti-spam filters.

When Exclaimer Anti-spam is enabled and filtering email messages, the anti-spam chain processes all features first. Features are only used for configuration purposes, as follows:

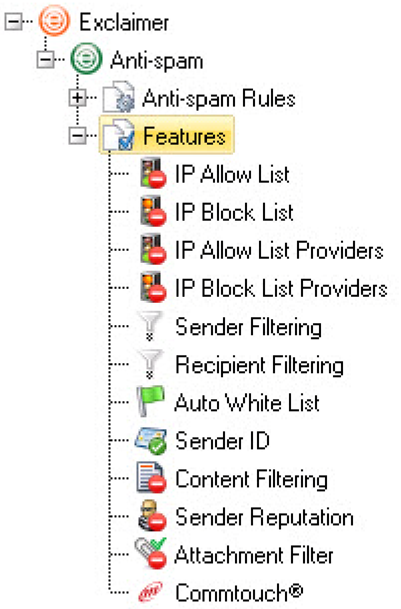
Feature	Summary
IP allow list	Maintain a list of IP addresses that are always allowed to connect to and transmit email messages to your server.
IP block list	Maintain a list of IP addresses that are known to be 'unsafe'. For further information please see page 132.
IP allow list providers	Configure IP allow list provider services to access third party lists of 'safe' IP addresses. For further information please see page 141.
IP block list providers	Configure IP block list provider services to access third party lists of 'unsafe' IP addresses. For further information please see page 149.
Sender filtering	Configure the sender block list [pg.67] and specify whether messages from blank senders should be blocked. For further information please see page 157.
Recipient filtering	Specify recipients for whom email messages will not be accepted. For further information please see page 161.
Auto white list	Specify whether any recipients of external messages sent from your organization should be added to a white list automatically. For further information please see page 164.
Sender ID	Configure the sender ID filter to check for spoof emails (including enable/disable options and 'blanket' actions to be taken for spoofed domains). For further information please see page 166.
Content filtering	Specify actions for messages at given Spam Confidence Level (SCL) thresholds, together with a list of allowed/blocked words and phrases for your organization. For further information please see page 170.
Sender reputation	Configure the sender reputation filter to calculate a Sender Reputation Level (SRL) i.e. - to determine the likelihood of their messages being spam. For further information please see page 177.
Attachment filter	Define actions to be taken with email messages containing attachments of a given file or content type. For further information please see page 182.
Commtouch	Enable/disable Commtouch classification [pg.106] on your system and set/check connectivity for this service. For further information please see page 191.

Once all features have been processed and any required actions have been applied, Exclaimer Anti-spam rules [pg.63] are processed. Rules provide straightforward, intuitive access to settings that are likely to be changed on a more regular basis, and to set additional 'belt and braces' options which are specific to Exclaimer Anti-spam.

Changing **features** may set your deployment mode [pg.58] to **custom**. If you have made changes and wish to revert to a standard deployment mode, you can simply select one of the standard options. If you do revert to a standard mode of deployment, any changes made to your white/block list **rules** will **not** be affected. However, any changes made to **features** will be cleared and reset to default values.

Accessing Features

Within Exclaimer Anti-spam, features are accessed from the Anti-spam branch of the Exclaimer console tree [pg.34]:


Exclaimer
Anti-spam
Anti-spam Rules
Features
IP Allow List
IP Block List
IP Allow List Providers
IP Block List Providers
Sender Filtering
Recipient Filtering
Auto White List
Sender ID
Content Filtering
Sender Reputation
Attachment Filter
Commtouch®

From here, all existing features are displayed; you can select any feature to display information and options. Available features include:

- IP allow list [pg.123]
- IP block list [pg.132]
- IP allow list providers [pg.141]
- IP block list providers [pg.149]
- Sender filtering [pg.157]
- Recipient filtering [pg.161]
- Auto white list [pg.164]
- Sender ID [pg.166]
- Content filtering [pg.170]
- Sender reputation [pg.177]
- Attachment filter [pg.182]
- Commtouch [pg.191]

IP Allow List

An Internet Protocol address (IP address) is a numeric label (used for identification and addressing) assigned to each device in a computer network that uses the Internet Protocol for communication.

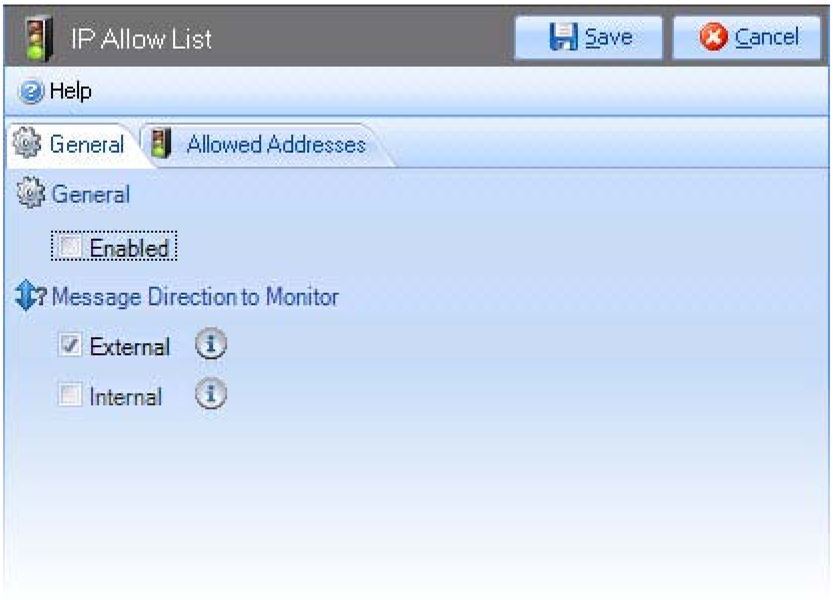
The IP allow list feature is used to enter IP addresses that are always allowed to connect to and transmit email messages to your server - i.e. IP addresses that are known to be 'safe'.

When adding IP addresses to the allow list, you can add a single IP address [pg.127], an IP address and mask [pg.128] or a range of IP addresses [pg.129].

If you have specific email addresses and/or domains that you wish to 'always allow', you can use the **sender white list rule** to add them quickly and easily.

General

General options are used to define basic settings for the IP allow list feature:



□ Enabled

Message Direction to Monitor

☑ External

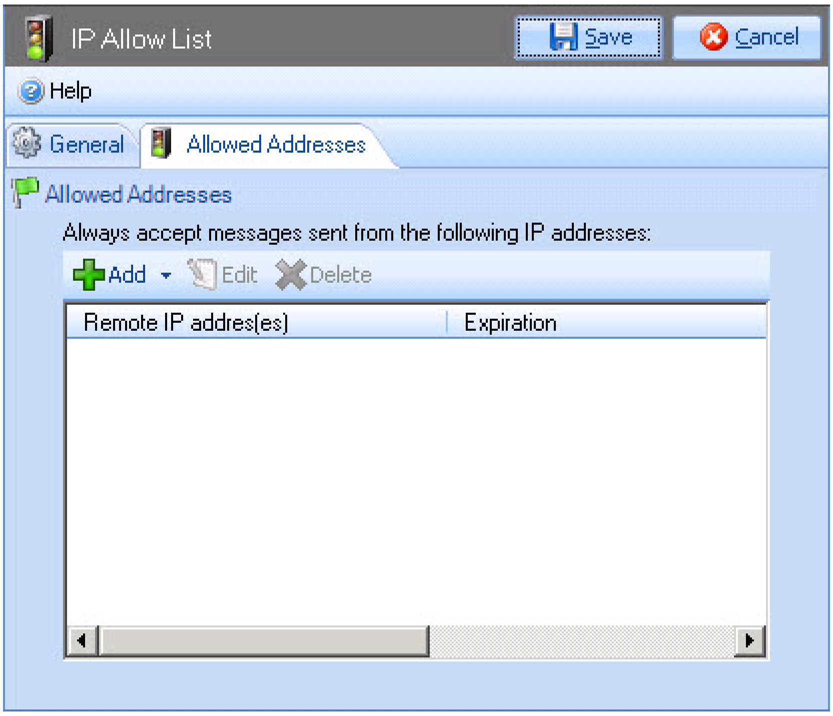
□ Internal

These settings are summarized below:

Option	Summary
Enabled	To enable the IP allow list, ensure that the enabled check box is ticked. If this option is not enabled, both the IP allow list feature and the sender white list rule [pg.77] will be disabled.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Allowed Addresses

The allowed addresses tab is used to enter IP addresses that are always allowed to connect to and transmit email messages to your server - i.e. IP addresses that are known to be 'safe':



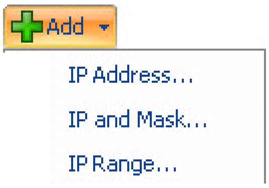
IP addresses are organized in the order in which they are added. You can add a single IP address [pg.127], an IP address and mask [pg.128] or an IP range [pg.129]. You can also edit [pg.130] and delete [pg.131] existing IP addresses as required.

If you have specific email addresses and/or domains that you wish to 'always allow', you can use the **sender white list rule** to add them quickly and easily.

Adding an Allowed IP Address

To add a new allowed IP address, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list branch.
3. Select the allowed addresses tab.
4. Click the add button to display available add options:

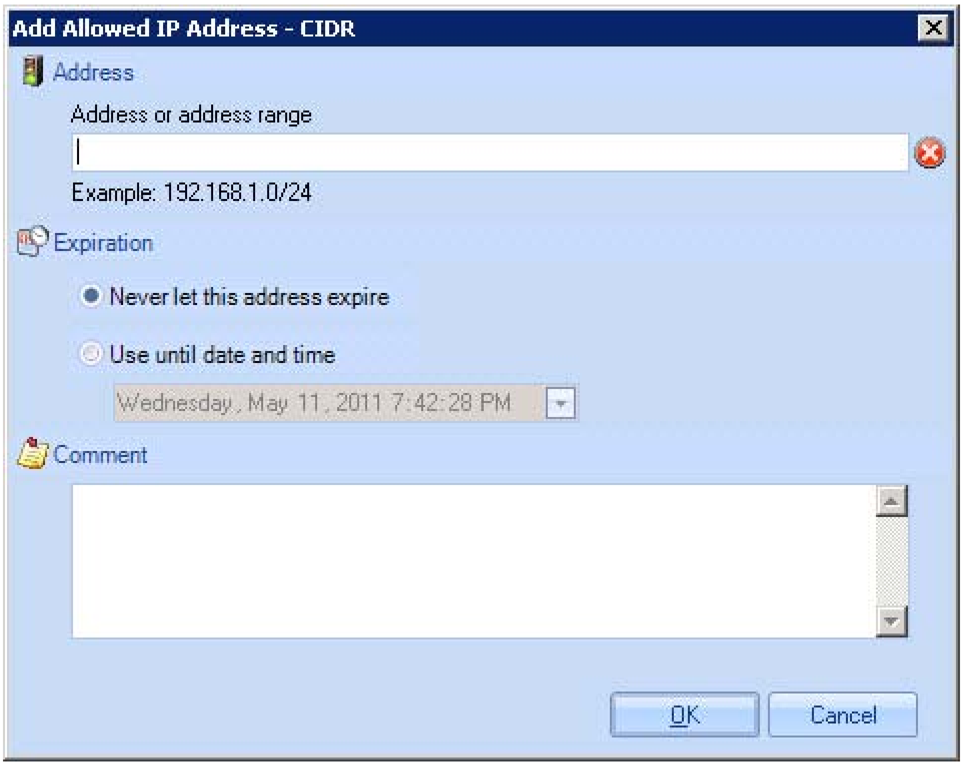


5. Select the required option and complete IP address [pg.127], IP and mask [pg.128] or IP range [pg.129] settings as required.
6. Click the save button (at the top of the window) to save changes.

Please refer to the following sections for further information about options for adding an **IP address**, **IP and mask** and an **IP range**.

Single IP Address Options

When you choose to add a single IP address, the add allowed IP address - CIDR window is displayed:



Add Allowed IP Address - CIDR
Address
Address or address range
Example: 192.168.1.0/24
Expiration
● Never let this address expire
○ Use until date and time
Wednesday , May 11, 2011 7:42:28 PM
Comment
OK
Cancel

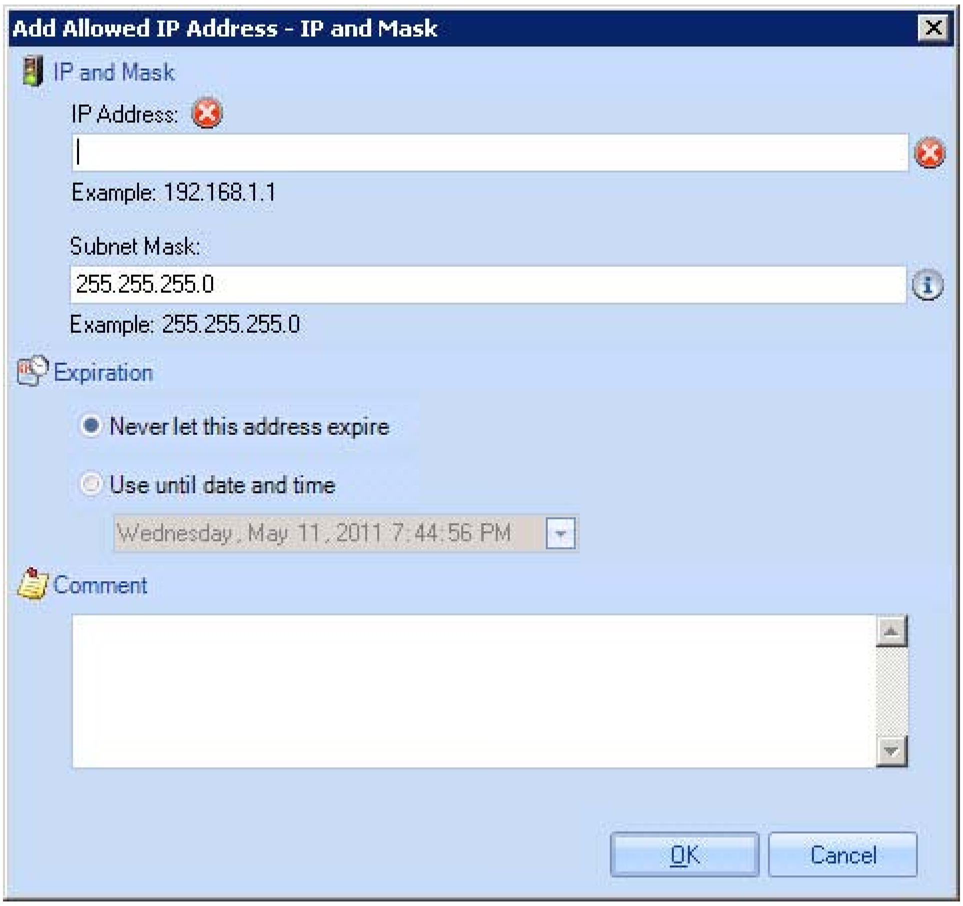
These settings are summarized below:

Option	Summary
Address or address range	Type the required IP address. You can enter a single IP address, or specify a range of addresses using CIDR notation - for example: 192.168.0.0/24. If you are not confident entering a range of addresses in this way, you can use the IP range [pg.129] option instead.
Expiration	If you wish to allow this IP address indefinitely, select the never let this address expire radio button. Alternatively, you can set an expiry date by selecting the use until date and time radio button and choosing the required date from the calendar.
Comment	Use the comment field to enter any notes regarding this IP address.

For detailed information about any of these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb125225.aspx.)

IP Address and Mask Options

When you choose to add an IP and mask, the add allowed IP address - IP and mask window is displayed:



Add Allowed IP Address - IP and Mask

IP and Mask

IP Address:

Example: 192.168.1.1

Subnet Mask: 255.255.255.0

Example: 255.255.255.0

Expiration

● Never let this address expire

○ Use until date and time

Wednesday, May 11, 2011 7:44:56 PM

Comment

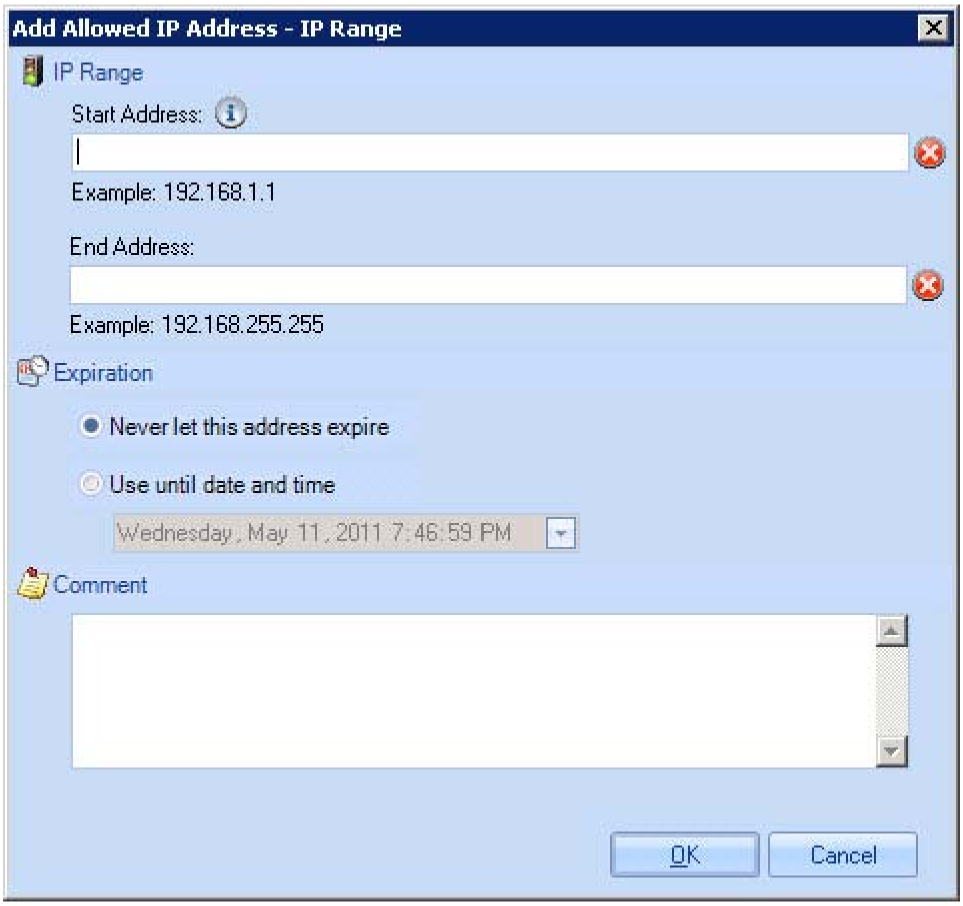
These settings are summarized below:

Option	Summary
IP Address	Type the required IP address.
Subnet mask	A subnet is part of a network that shares a common address component. On TCP/IP (Transmission Control Protocol/Internet Protocol) networks, a subnet is defined as all devices whose IP address has the same prefix. For example, all devices with an IP address that starts with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons and it is done using a subnet mask. Enter the required subnet mask here.
Expiration	If you wish to allow this IP address indefinitely, select the never let this address expire radio button. Alternatively, you can set an expiry date by selecting the use until date and time radio button and choosing the required date from the calendar.
Comment	Use the comment field to enter any notes regarding this IP address.

For detailed information about any of these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb125225.aspx.)

IP Range Options

When you choose to add an IP range, the add allowed IP address - IP range window is displayed:



Add Allowed IP Address - IP Range

IP Range

Start Address:

Example: 192.168.1.1

End Address:

Example: 192.168.255.255

Expiration

● Never let this address expire

○ Use until date and time

Wednesday , May 11 , 2011 7:46:59 PM

Comment

These settings are summarized below:

Option	Summary
Start address	Type the first IP address in the range (this address will be included).
End address	Type the last IP address in the range (this address will be included).
Expiration	If you wish to allow this IP address range indefinitely, select the never let this address expire radio button. Alternatively, you can set an expiry date by selecting the use until date and time radio button and choosing the required date from the calendar.
Comment	Use the comment field to enter any notes regarding this IP address.

For detailed information about any of these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb125225.aspx.)

Editing an Allowed IP Address

To edit an existing IP address, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list branch.
3. Select the allowed addresses tab.
4. Select the required entry in the list.
5. Click the edit button to open the edit allowed IP address window. The content of this window will vary dependent upon whether you have chosen to edit a single IP address [pg.127], an IP address and mask [pg.128], or a range of IP addresses [pg.129].
6. Make changes as required.
7. Click OK to update the entry and exit back to the allowed addresses tab.
8. Click the save button (at the top of the window) to save changes.

> For detailed information about any of these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb125225.aspx.)

Deleting an Allowed IP Address

To delete an existing IP address, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list branch.
3. Select the allowed addresses tab.
4. Select the required entry in the list.
5. Click the delete button. You are asked if you are sure that you wish to remove the selected entry.
6. If you are satisfied that the correct IP address has been selected, click yes to complete the deletion and exit back to the allowed addresses tab.
7. Click the save button (at the top of the window) to save changes.

If required, you can delete a range of entries at the same time. To select a range of entries that are organised contiguously, press and hold down the **SHIFT** key and then select the first and last entries to be removed. All items between (and including) these points will be selected.

To select a range of entries that are not organised contiguously, press and hold down the **CTRL** key and then select required entries.

IP Block List

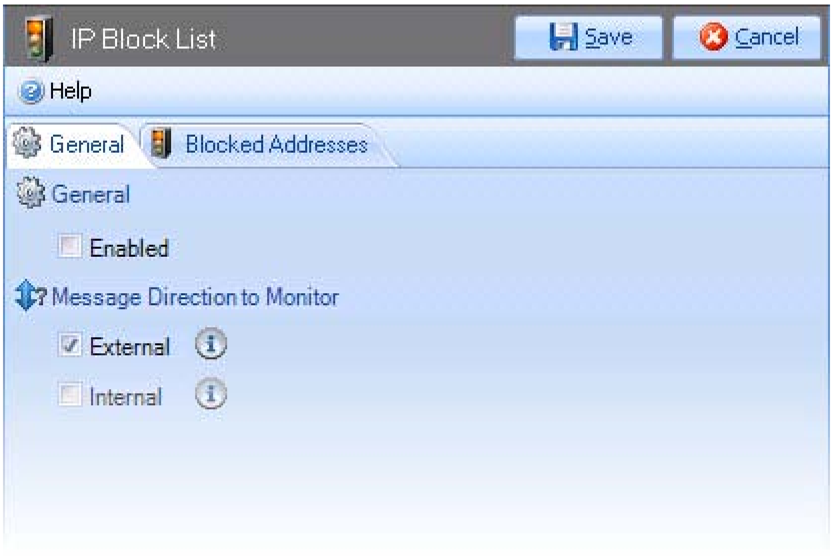
An Internet Protocol address (IP address) is a numeric label (used for identification and addressing) assigned to each device in a computer network that uses the Internet Protocol for communication. The IP block list feature is used to enter IP addresses that are never allowed to connect to your server.

When adding IP addresses to the block list, you can add a single IP address [pg.136], an IP address and mask [pg.137] or a range of IP addresses [pg.138].

IP addresses may also be added automatically via the sender reputation feature [pg.177]. If you have specific email addresses and/or domains that you wish to block, you can use the sender block list [pg.67] rule to add them quickly and easily.

General

General options are used to define basic settings for the IP block list feature:



□ Enabled

Message Direction to Monitor

☑ External

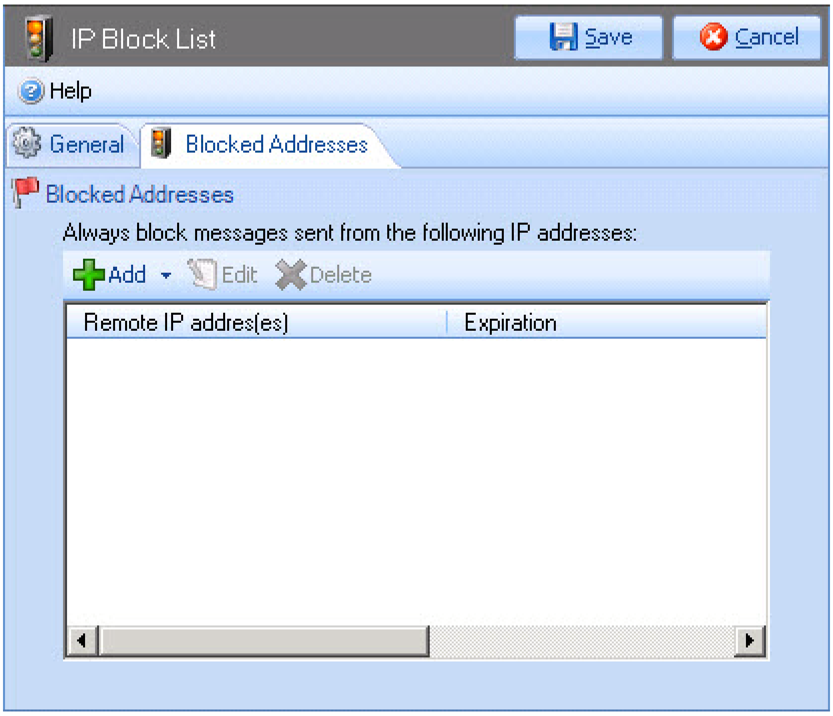
□ Internal

These settings are summarized below:

Option	Summary
Enabled	To enable the IP block list feature, ensure that the enabled check box is ticked. If this option is not enabled, both the IP block list feature and the sender block list rule [pg.67] will be disabled.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Blocked Addresses

The blocked addresses tab is used to enter IP addresses that are never allowed to transmit email messages to your server - i.e. IP addresses that are known to be associated with spam:



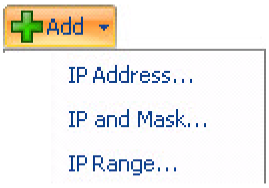
IP addresses are organized in the order in which they are added. You can add a single IP address [pg.136], an IP address and mask [pg.137] or an IP range [pg.138]. You can also edit [pg.139] and delete [pg.140] existing IP addresses as required.

IP addresses may also be added automatically via the sender reputation feature [pg.177]. If you have specific email addresses and/or domains that you wish to block, you can use the sender block list [pg.67] rule to add them quickly and easily.

Adding a Blocked IP Address

To add a new blocked IP address, follow the steps below:

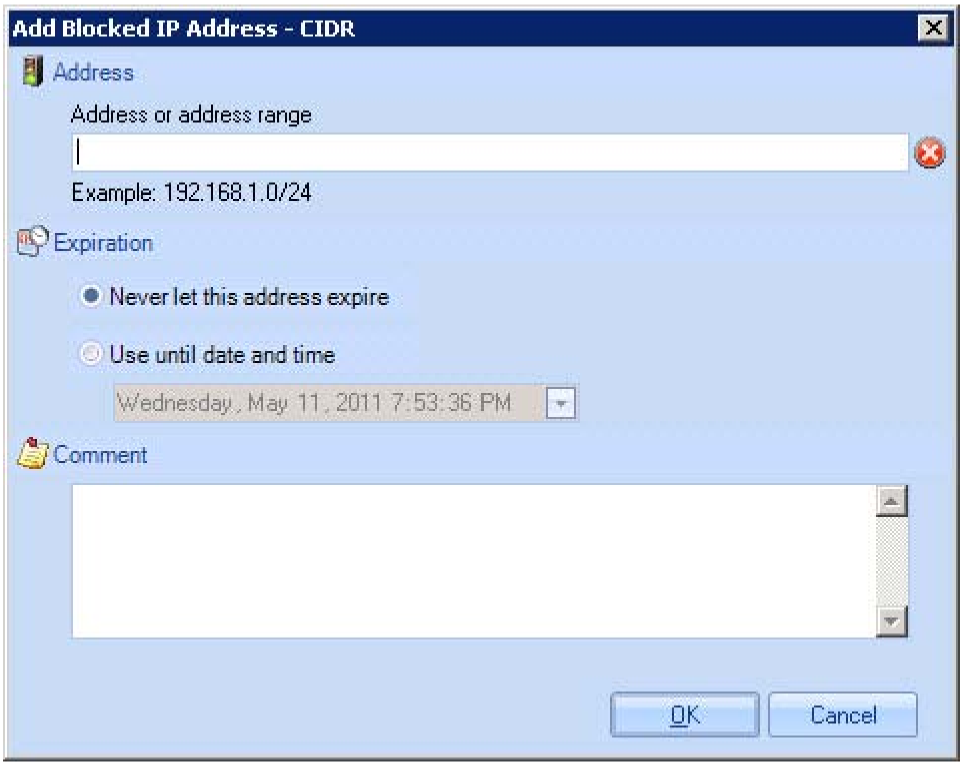
1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list branch.
3. Select the blocked addresses tab.
4. Click the add button to display available add options:



5. Select the required option and complete single IP address [pg.136], IP address and mask [pg.137] or range of IP addresses [pg.138] settings as required.
6. Click the save button (at the top of the window) to save changes.

Single IP Address Options

When you choose to add a single IP address, the add blocked IP address - CIDR window is displayed:



Add Blocked IP Address - CIDR

Address

Address or address range

Example: 192.168.1.0/24

Expiration

● Never let this address expire

○ Use until date and time

Wednesday, May 11, 2011 7:53:36 PM

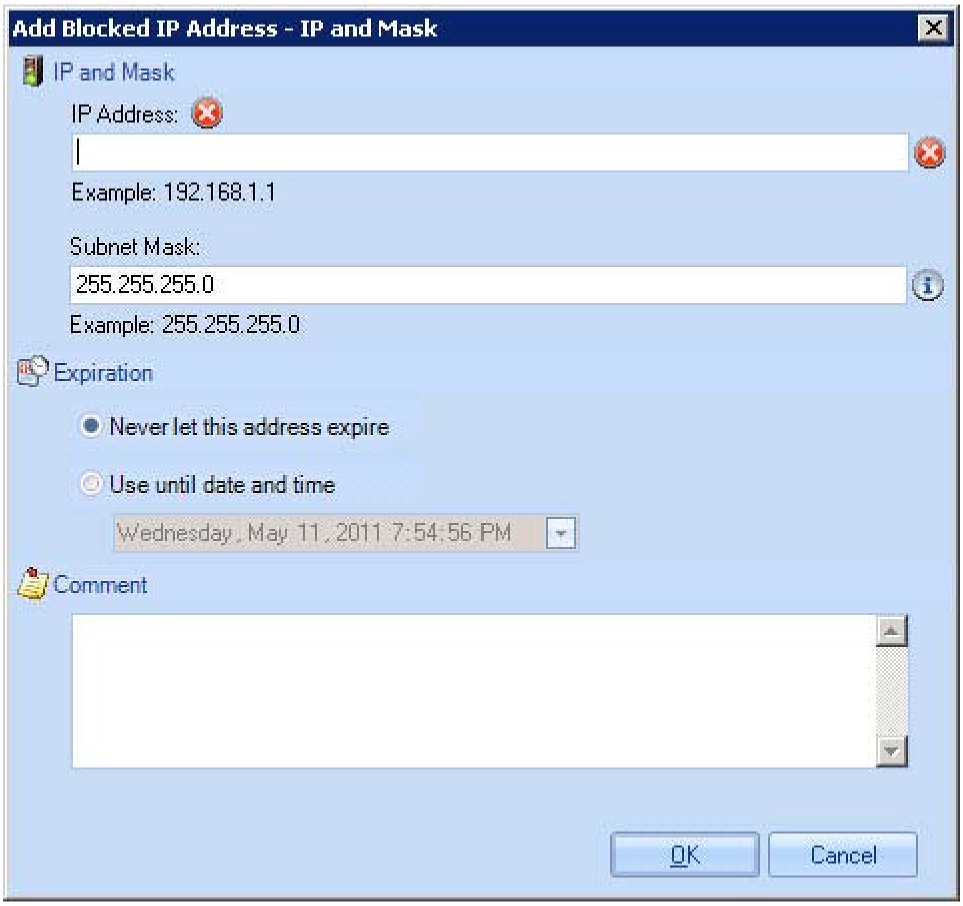
Comment

These settings are summarized below:

Option	Summary
Address or address range	Type the required IP address. You can enter a single IP address, or specify a range of addresses using CIDR notation - for example: 192.168.0.0/24. If you are not confident entering a range of addresses in this way, you can use the IP range [pg.138] option instead.
Expiration	If you wish to block this IP address indefinitely, select the never let this address expire radio button. Alternatively, you can set an expiry date by selecting the use until date and time radio button and choosing the required date from the calendar.
Comment	Use the comment field to enter any notes regarding this IP address - for example, you might wish to note why the address is blocked or why an expiry date has been set.

IP Address and Mask Options

When you choose to add an IP and mask, the add blocked IP address - IP and mask window is displayed:



Add Blocked IP Address - IP and Mask

IP and Mask

IP Address:

Example: 192.168.1.1

Subnet Mask: 255.255.255.0

Example: 255.255.255.0

Expiration

● Never let this address expire

○ Use until date and time

Wednesday , May 11, 2011 7:54:56 PM

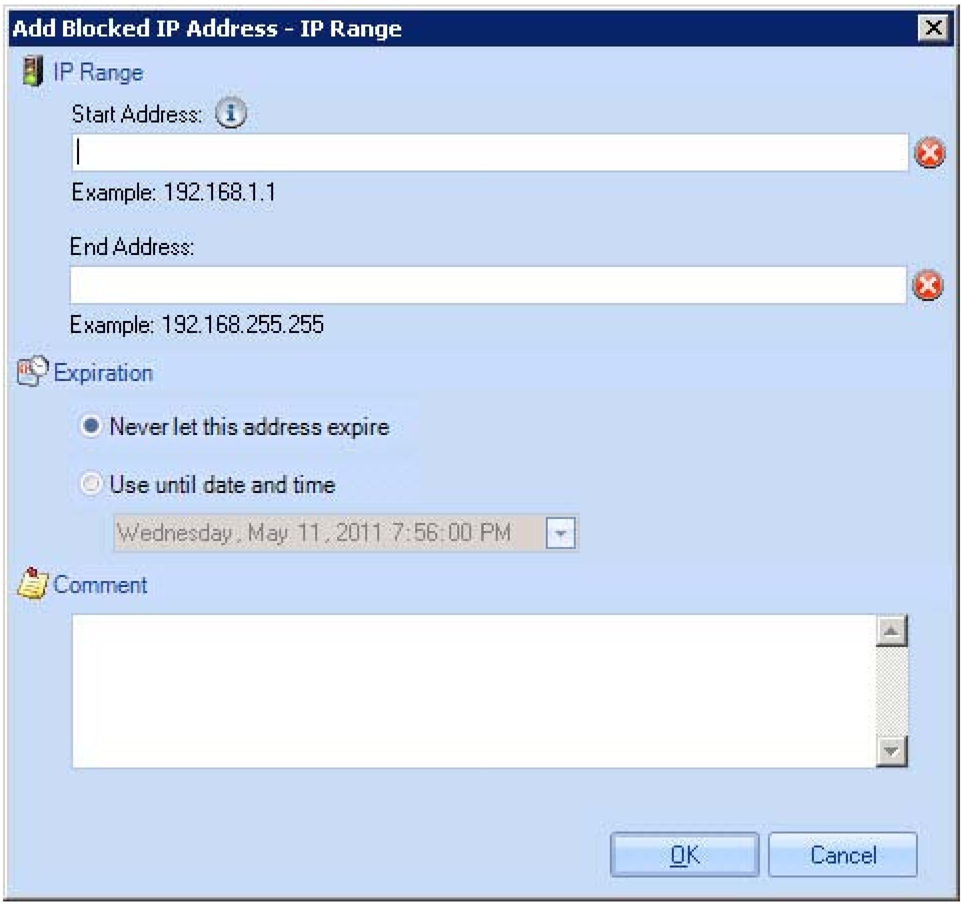
Comment

These settings are summarized below:

Option	Summary
IP Address	Type the required IP address.
Subnet mask	A subnet is part of a network that shares a common address component. On TCP/IP (Transmission Control Protocol/Internet Protocol) networks, a subnet is defined as all devices whose IP address has the same prefix. For example, all devices with an IP address that starts with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons and it is done using a subnet mask. Enter the required subnet mask here.
Expiration	If you wish to block this IP address indefinitely, select the never let this address expire radio button. Alternatively, you can set an expiry date by selecting the use until date and time radio button and choosing the required date from the calendar.
Comment	Use the comment field to enter any notes regarding this IP address - for example, you might wish to note why the address is blocked or why an expiry date has been set.

IP Range Options

When you choose to add an IP range, the add blocked IP address - IP range window is displayed:



Add Blocked IP Address - IP Range

IP Range

Start Address:

Example: 192.168.1.1

End Address:

Example: 192.168.255.255

Expiration

● Never let this address expire

○ Use until date and time

Wednesday , May 11, 2011 7:56:00 PM

Comment

These settings are summarized below:

Option	Summary
Start address	Type the first IP address in the range (this address will be included).
End address	Type the last IP address in the range (this address will be included).
Expiration	If you wish to block this IP address range indefinitely, select the never let this address expire radio button. Alternatively, you can set an expiry date by selecting the use until date and time radio button and choosing the required date from the calendar.
Comment	Use the comment field to enter any notes regarding this IP address range - for example, you might wish to note why the range is blocked or what the range represents.

For detailed information about any of these options you may wish to view articles on the Microsoft Technet website http://technet.microsoft.com/en-us/library/bb124912.aspx).

Editing a Blocked IP Address

To edit an existing IP address, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list branch.
3. Select the blocked addresses tab.
4. Select the required entry in the list.
5. Click the edit button to open the edit blocked IP address window. The content of this window will vary dependent upon whether you have chosen to edit a single IP address [pg.136], an IP address and mask [pg.137] or a range of IP addresses [pg.138].
6. Make changes as required.
7. Click OK to update the entry and exit back to the blocked addresses tab.
8. Click the save button (at the top of the window) to save changes.

For detailed information about any of these options you may wish to view articles on the Technet website http://technet.microsoft.com/en-us/library/bb124912.aspx).

Deleting a Blocked IP Address

To delete an existing IP address, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list branch.
3. Select the blocked addresses tab.
4. Select the required entry in the list.
5. Click the delete button. You are asked if you are sure that you wish to remove the selected entry.
6. If you are satisfied that the correct IP address has been selected, click yes to complete the deletion and exit back to the blocked addresses tab.
7. Click the save button (at the top of the window) to save changes.

If required, you can delete a range of entries at the same time. To select a range of entries that are organised contiguously, press and hold down the **SHIFT** key and then select the first and last entries to be removed. All items between (and including) these points will be selected.

To select a range of entries that are not organised contiguously, press and hold down the **CTRL** key and then select required entries.

IP Allow List Providers

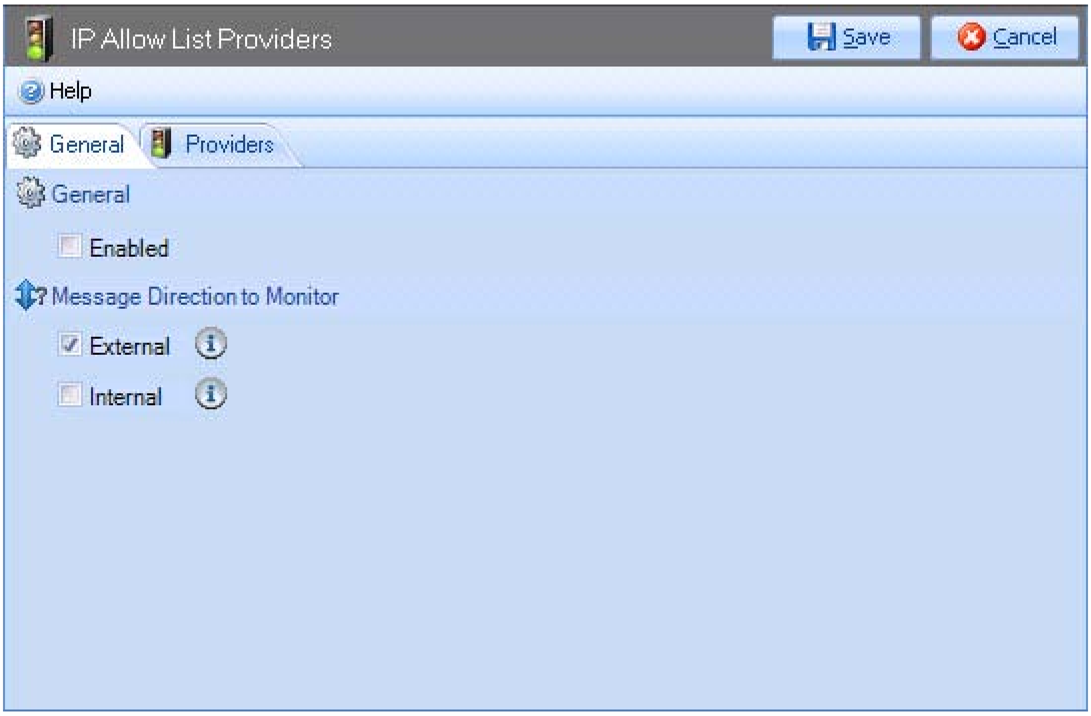
Within Exclaimer Anti-spam, you can maintain your own IP allow list [pg.123], but IP allow list providers take this a step further.

IP allow list providers are third party organizations who maintain lists of IP addresses that are known to be 'safe' - i.e. they are not associated with any spam activity. When an IP allow list provider returns a match for an IP address, it is an indication that the sender's IP address is safe and the message continues to the next stage in the anti-spam chain.

The IP allow list providers feature includes two tabs - general [pg.142] (used to define basic settings) and providers [pg.143] (used to configure IP allow list provider services).

General

General options are used to define basic settings for the IP allow list providers feature:



General

□ Enabled

Message Direction to Monitor

☑ External

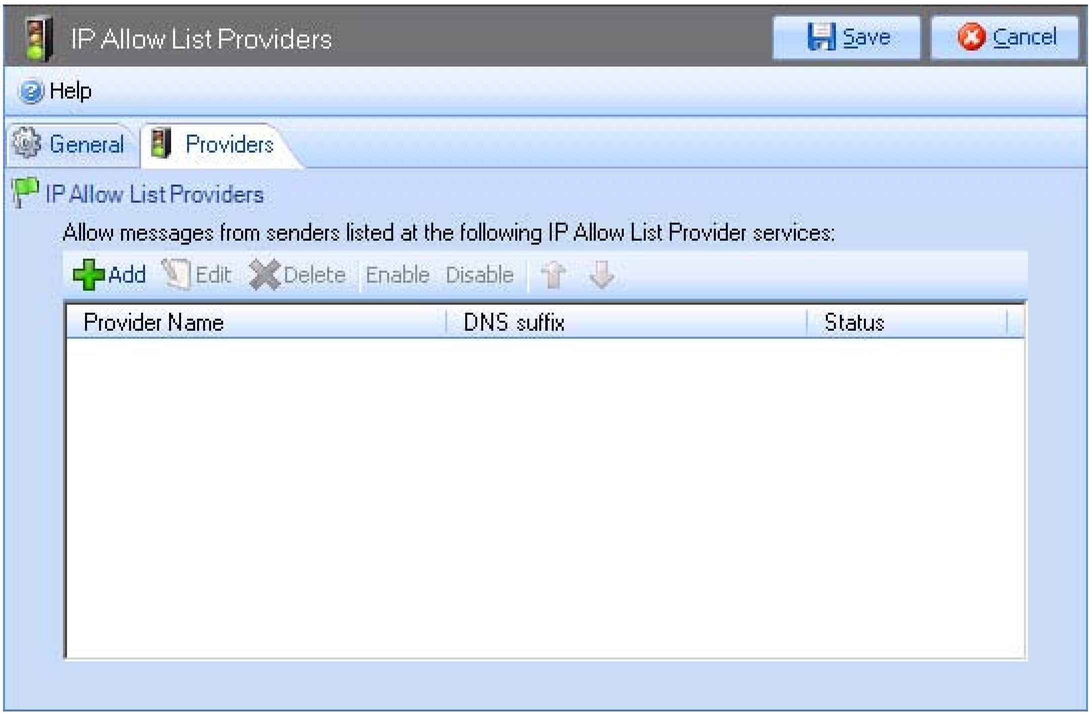
□ Internal

These settings are summarized below:

Option	Summary
Enabled	To enable the IP allow list providers, ensure that the enabled check box is ticked.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Providers

The providers tab is used to manage the IP allow list provider services:



Allow messages from senders listed at the following IP Allow List Provider services:

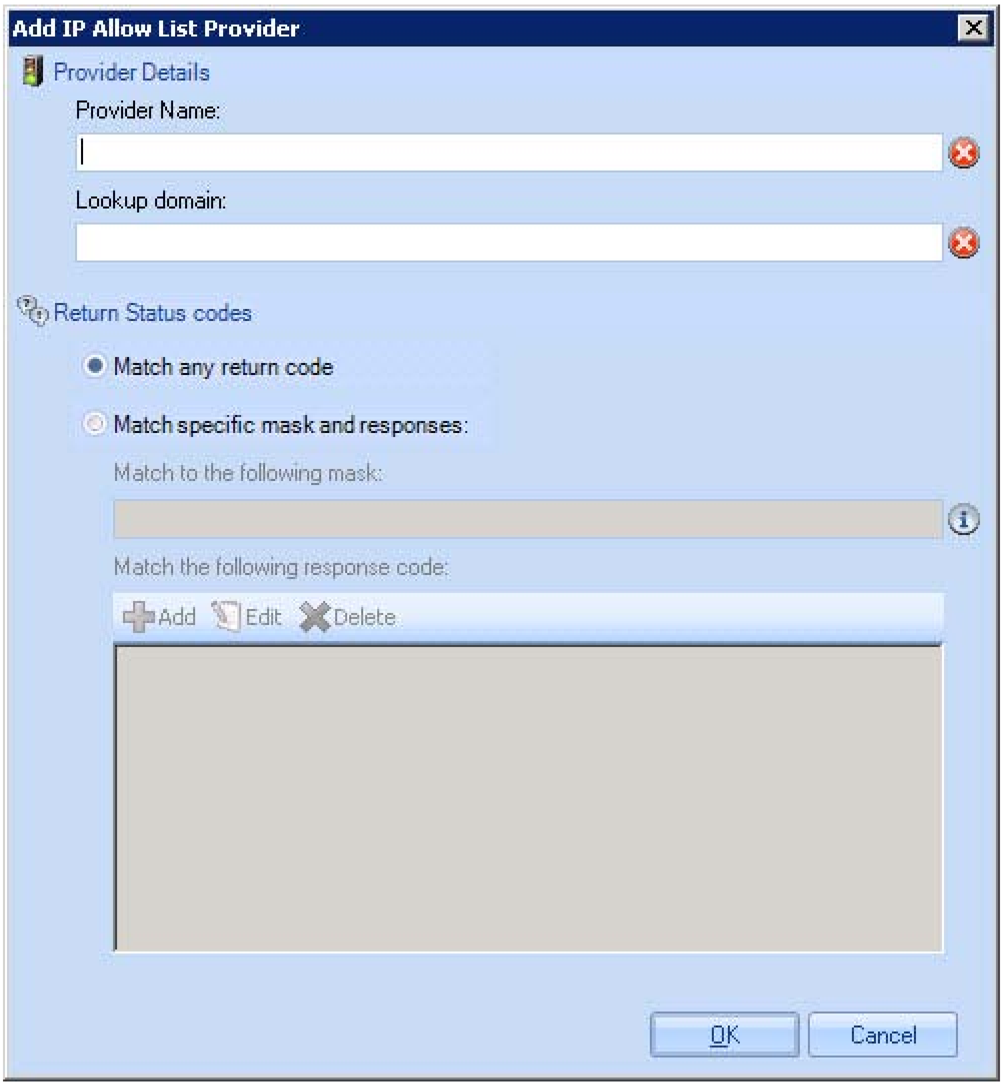
Provider Name	DNS suffix	Status

From here you can add [pg.144], edit [pg.146], delete [pg.147] or enable/disable [pg.148] providers. You can also use up/down arrow buttons to change the order in which providers are listed. To optimize performance you are advised to put the most reliable providers first - if an IP allow list match is made from one provider the system stops querying other provider services.

Adding an Allow List Provider

To add a new IP allow list provider, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list providers branch.
3. Select the providers tab.
4. Click the add button to open the add IP allow list provider window:



Add IP Allow List Provider

Provider Details

Provider Name:

Lookup domain:

Return Status codes

● Match any return code

○ Match specific mask and responses:

Match to the following mask:

Match the following response code:

5. Enter details for the provider using the table below as a guide:

Option	Summary
Provider name	Type the name of the IP allow list provider service. This name is for your own use to identify the provider.
Look up domain	Type the domain name to be queried for updated IP allow list information. This information should be supplied by your chosen allow list provider.
Match any return code	Select this option if you wish to treat **any** returned IP address status codes (from the IP allow list provider) as a match.
Match specific mask and responses	Select this option if you wish to treat only specified IP address status codes (from the IP allow list provider) as a match. First, enter the required mask and then click the add button to enter the required response code. You can also edit and delete response codes using edit and delete buttons respectively.

For detailed information about these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb123964.aspx).

6. Click OK to add the entry to the list and exit back to the providers tab.

7. Add further providers as required.

8. Click the save button (at the top of the window) to save changes.

To optimize performance you are advised to put the most reliable providers first - if an **IP allow list** match is made from one provider the system stops querying other provider services.

Editing an Allow List Provider

To edit an existing IP allow list provider, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list providers branch.
3. Select the providers tab.
4. Select the required entry in the list.
5. Click the edit button to open the edit allow list provider window.
6. Make changes as required using the table below as a guide:

Option	Summary
Provider name	Type the name of the IP allow list provider service. This name is for your own use to identify the provider.
Look up domain	Type the domain name to be queried for updated IP allow list information. This information should be supplied by your chosen allow list provider.
Match any return code	Select this option if you wish to treat **any** returned IP address status codes (from the IP allow list provider) as a match.
Match specific mask and responses	Select this option if you wish to treat only specified IP address status codes from the IP allow list provider) as a match. First, enter the required mask and then click the add button to enter the required response code. You can also edit and delete response codes using edit and delete buttons respectively.

For detailed information about these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb123964.aspx).

7. Click OK to update the entry and exit back to the providers tab.
8. Click the save button (at the top of the window) to save changes.

You can change all settings for an existing provider except the **provider name** (since this is used throughout the system). If you need to change the **provider name** you should delete the provider and enter the details again with the correct name.

Deleting an Allow List Provider

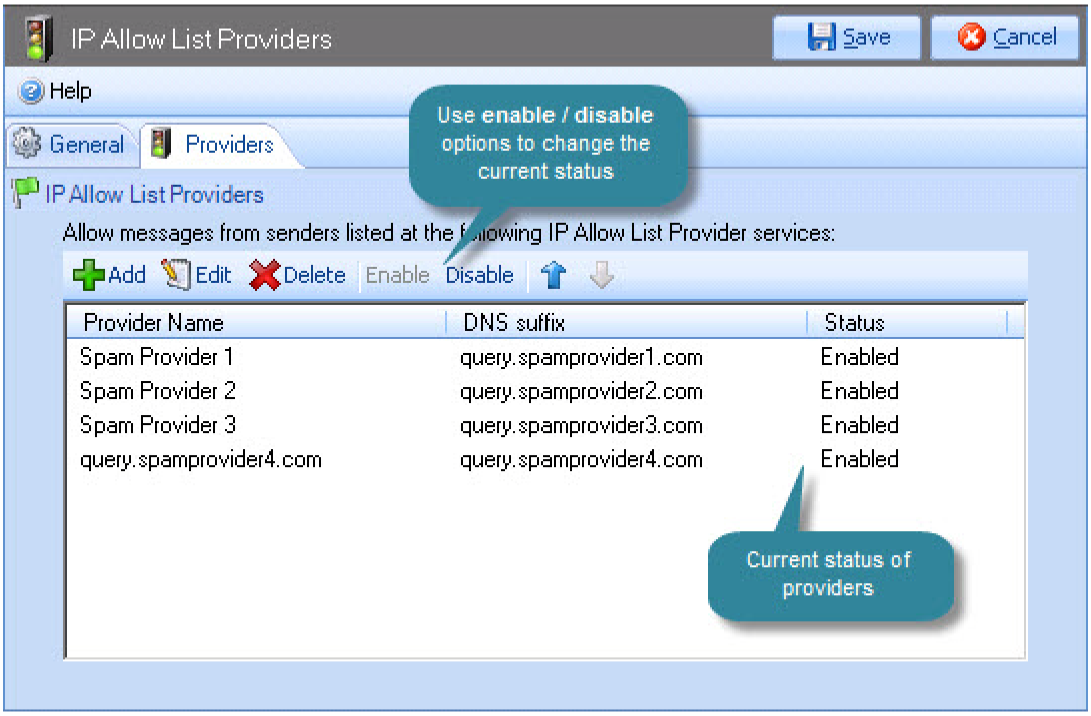
To delete an existing IP allow list provider, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list providers branch.
3. Select the providers tab.
4. Select the required entry in the list.
5. Click the delete button. You are asked if you are sure that you wish to remove the selected entry.
6. If you are satisfied that the correct provider has been selected, click yes to complete the deletion and exit back to the providers tab.
7. Click the save button (at the top of the window) to save changes.

Enabling/Disabling an Allow List Provider

If you wish to stop using a particular allow list provider but you do not wish to go as far as deleting [pg.147] it, you can use enable/disable options. To do this, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP allow list providers branch.
3. Select the providers tab.
4. Select the required entry in the list.
5. Click the edit button to open the edit allow list provider window. Here, you can see all existing providers and whether or not they are enabled or disabled.
6. Select the entry that you wish to change:



Allow messages from senders listed at the following IP Allow List Provider services:

Provider Name	DNS suffix	Status
Spam Provider 1	query.spamprovider1.com	Enabled
Spam Provider 2	query.spamprovider2.com	Enabled
Spam Provider 3	query.spamprovider3.com	Enabled
query.spamprovider4.com	query.spamprovider4.com	Enabled

7. If the entry is currently enabled, the disable button will be available on the toolbar. If the entry is currently disabled, the enable button is available. Select the appropriate button.
8. Click the save button (at the top of the window) to save changes.

IP Block List Providers

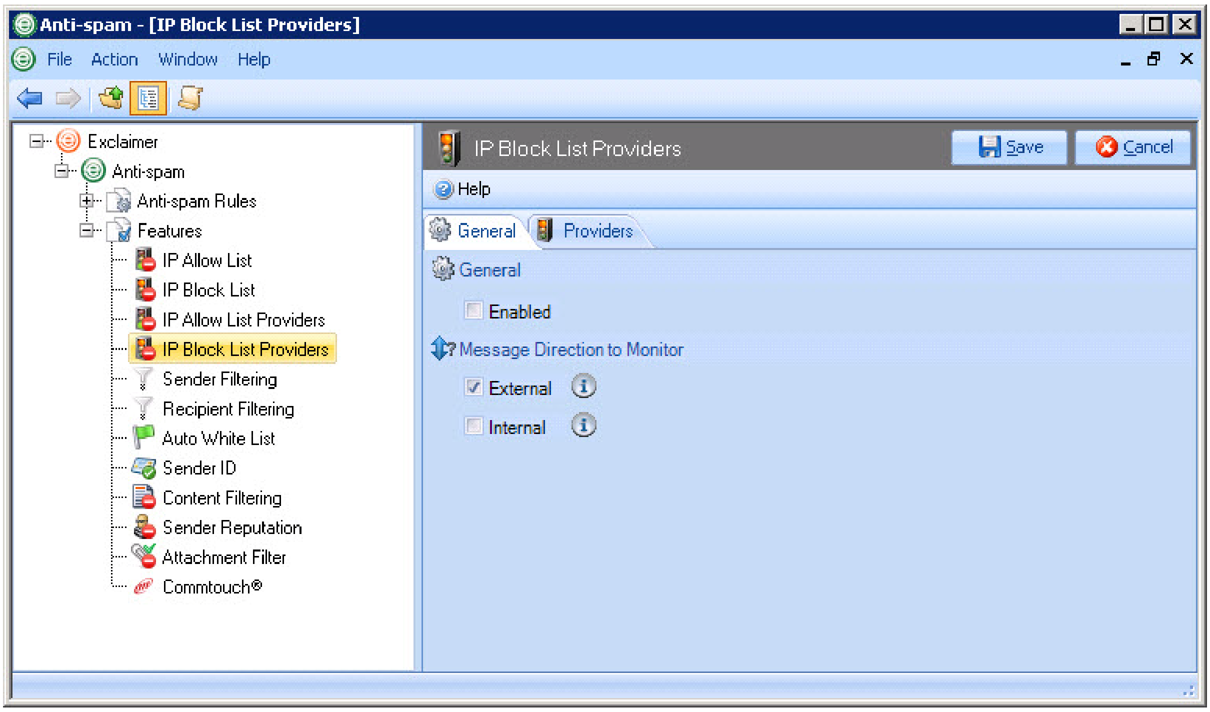
Within Exclaimer Anti-spam, you can maintain your own IP block list [pg.132], but IP block list providers take this a step further.

IP block list providers are third party organizations who maintain lists of IP addresses that are known to be associated with any spam activity. When an IP block list provider returns a match for an IP address, it is an indication that the sender's IP address is not safe and the message is blocked.

The IP block list providers feature includes two tabs - general [pg.150] (used to define basic settings) and providers [pg.151] (used to configure IP block list provider services).

General

General options are used to define basic settings for the IP block list providers feature:



□ Enabled

☑ External

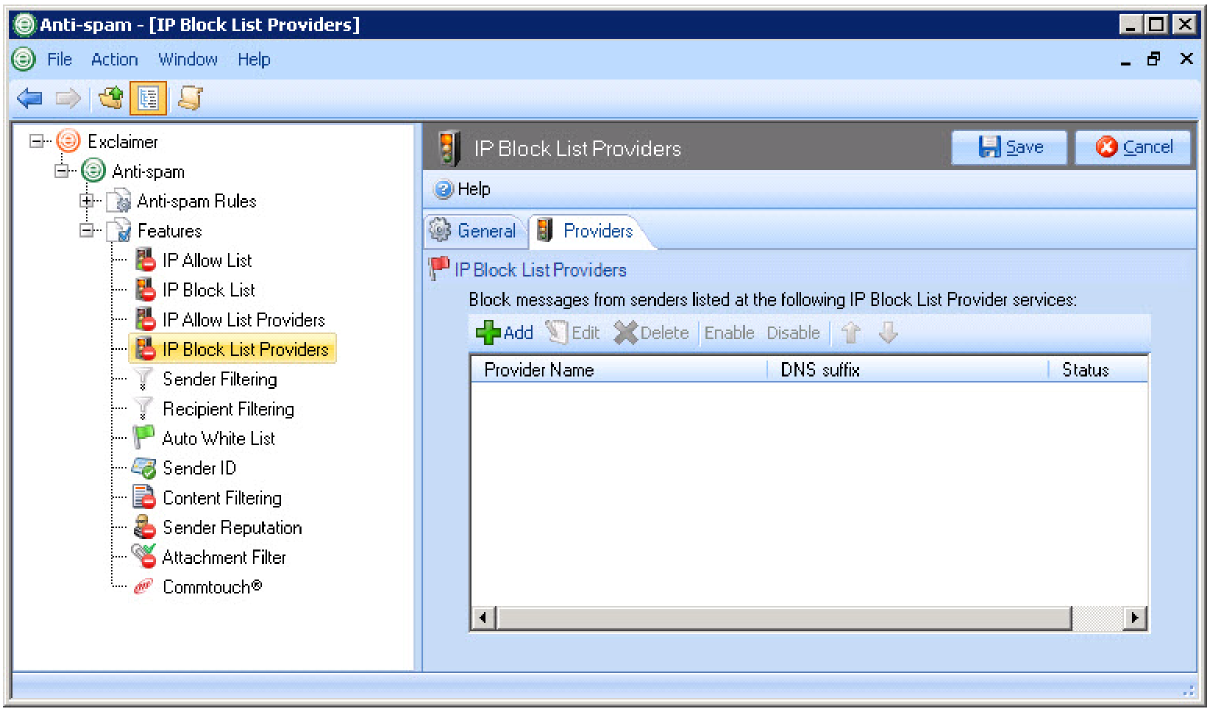
□ Internal

These settings are summarized below:

Option	Summary
Enabled	To enable the IP block list providers, ensure that the enabled check box is ticked.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Providers

The providers tab is used to manage the IP block list provider services:



Block messages from senders listed at the following IP Block List Provider services:

Provider Name	DNS suffix	Status

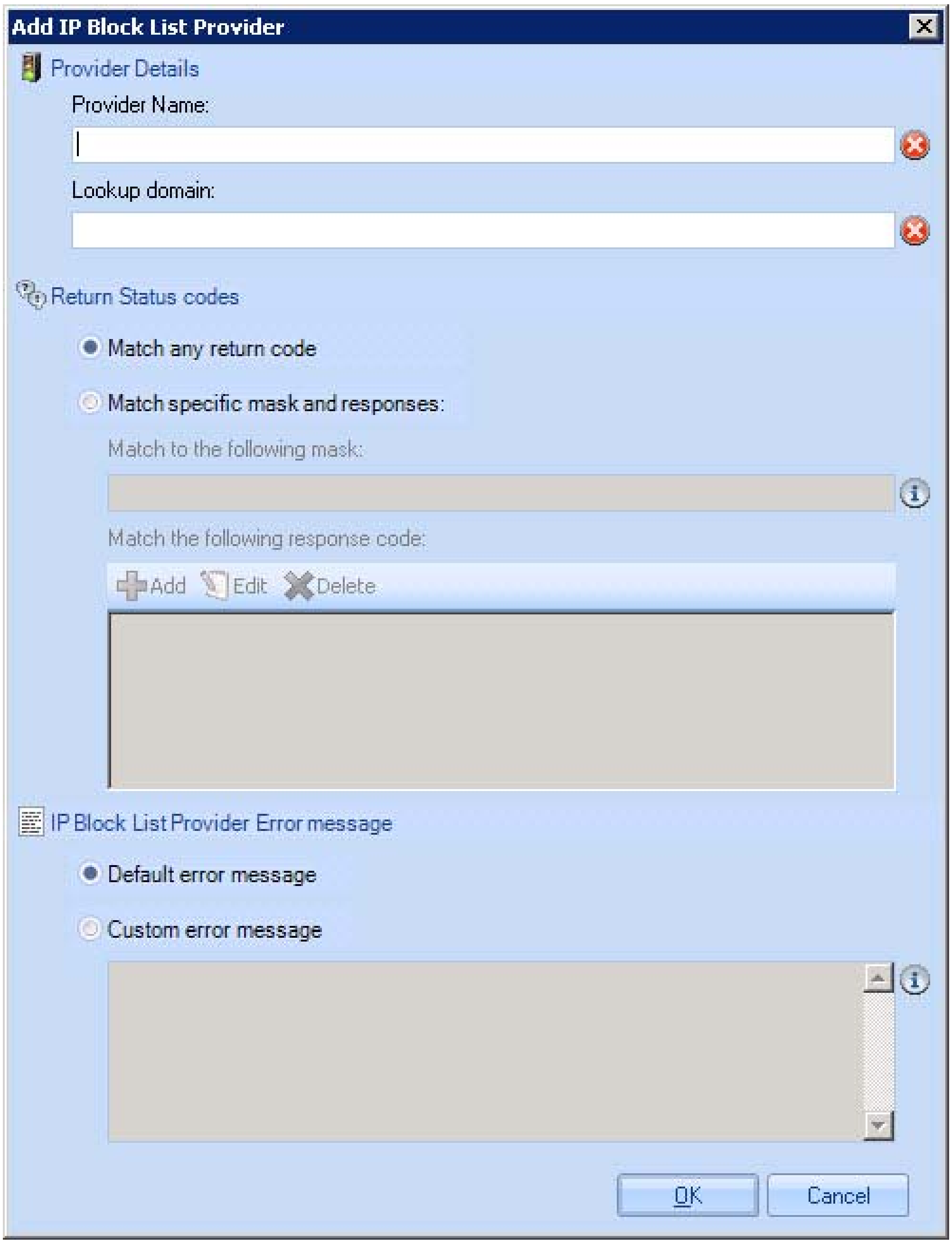
From here you can add [pg.152], edit [pg.154], delete [pg.155] or enable/disable [pg.156] providers. You can also use up/down arrow buttons to change the order in which providers are listed.

To optimize performance you are advised to put the most reliable providers first - if an IP block list match is made from one provider the system stops querying other provider services.

Adding a Block List Provider

To add a new IP block list provider, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list providers branch.
3. Select the providers tab.
4. Click the add button to open the add IP block list provider window:



Add IP Block List Provider

Provider Details

Provider Name:

Lookup domain:

Return Status codes

● Match any return code

○ Match specific mask and responses:

Match to the following mask:

Match the following response code:

IP Block List Provider Error message

● Default error message

○ Custom error message

5. Enter details for the provider using the table below as a guide:

Option	Summary
Provider name	Type the name of the IP block list provider service. This name is for your own use to identify the provider.
Look up domain	Type the domain name to be queried for updated IP block list information. This information should be supplied by your chosen block list provider.
Match any return code	Select this option if you wish to treat **any** returned IP address status codes (from the IP block list provider) as a match.
Match specific mask and responses	Select this option if you wish to treat only specified IP address status codes from the IP block list provider) as a match. First, enter the required mask and then click the add button to enter the required response code. You can also edit and delete response codes using edit and delete buttons respectively.
IP block list provider error message	If a message is blocked because the sender has been identified on a provider's block list, a message is returned to the sender's mail server. You can choose to use the default Exchange error message, or to send your own custom error message. This might be useful (for example) if you wish to specify format codes to help legitimate email senders work out why their email was blocked (e.g. The IP address %0 was rejected by black list %2).

For detailed information about these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/dd351199.aspx).

6. Click OK to add the entry to the list and exit back to the providers tab.

7. Add further providers as required.

8. Click the save button (at the top of the window) to save changes.

To optimize performance you are advised to put the most reliable providers first - if an **IP block list** match is made from one provider the system stops querying other provider services.

Editing a Block List Provider

To edit an existing IP block list provider, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list providers branch.
3. Select the providers tab.
4. Select the required entry in the list.
5. Click the edit button to open the edit block list provider window.
6. Make changes as required using the table below as a guide:

Option	Summary
Provider name	Type the name of the IP block list provider service. This name is for your own use to identify the provider.
Look up domain	Type the domain name to be queried for updated IP block list information. This information should be supplied by your chosen allow list provider.
Match any return code	Select this option if you wish to treat **any** returned IP address status codes (from the IP block list provider) as a match.
Match specific mask and responses	Select this option if you wish to treat only specified IP address status codes from the IP block list provider) as a match. First, enter the required mask and then click the add button to enter the required response code. You can also edit and delete response codes using edit and delete buttons respectively.
IP block list provider error message	If a message is blocked because the sender has been identified on a provider's block list, a message is returned to the sender's mail server. You can choose to use the default Exchange error message, or to send your own custom error message. This might be useful (for example) if you wish to specify format codes to help legitimate email senders work out why their email was blocked (e.g. The IP address %0 was rejected by black list %2).

For detailed information about these options you may wish to view articles on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/dd351199.aspx).

7. Click OK to update the entry and exit back to the providers tab.
8. Click the save button (at the top of the window) to save changes.

You can change all settings for an existing provider except the **provider name** (since this is used throughout the system). If you need to change the **provider name** you should delete the provider and enter the details again with the correct name.

Deleting a Block List Provider

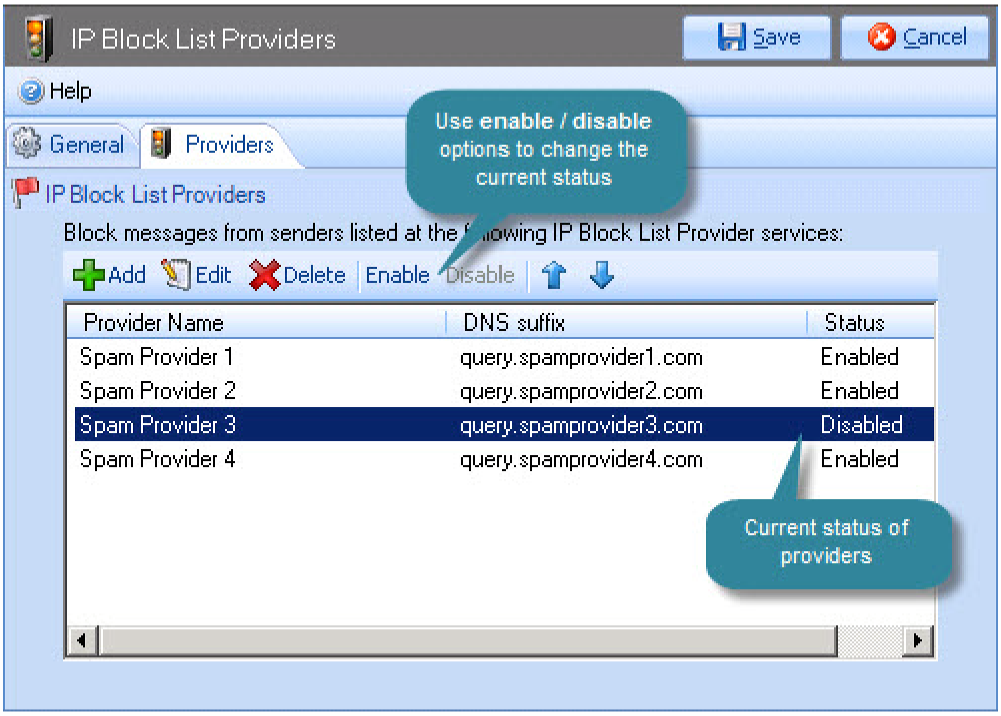
To delete an existing IP block list provider, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list providers branch.
3. Select the providers tab.
4. Select the required entry in the list.
5. Click the delete button. You are asked if you are sure that you wish to remove the selected entry.
6. If you are satisfied that the correct provider has been selected, click yes to complete the deletion and exit back to the providers tab.
7. Click the save button (at the top of the window) to save changes.

Enabling/Disabling a Block List Provider

If you wish to stop using a particular block list provider but you do not wish to go as far as deleting [pg.147] it, you can use enable/disable options. To do this, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the IP block list providers branch.
3. Select the providers tab.
4. Select the required entry in the list.
5. Click the edit button to open the edit block list provider window. Here, you can see all existing providers and whether or not they are enabled or disabled.
6. Select the entry that you wish to change:



Block messages from senders listed at the following IP Block List Provider services:

Provider Name	DNS suffix	Status
Spam Provider 1	query.spamprovider1.com	Enabled
Spam Provider 2	query.spamprovider2.com	Enabled
Spam Provider 3	query.spamprovider3.com	Disabled
Spam Provider 4	query.spamprovider4.com	Enabled

7. If the entry is currently enabled, the disable button will be available on the toolbar. If the entry is currently disabled, the enable button is available. Select the appropriate button.
8. Click the save button (at the top of the window) to save changes.

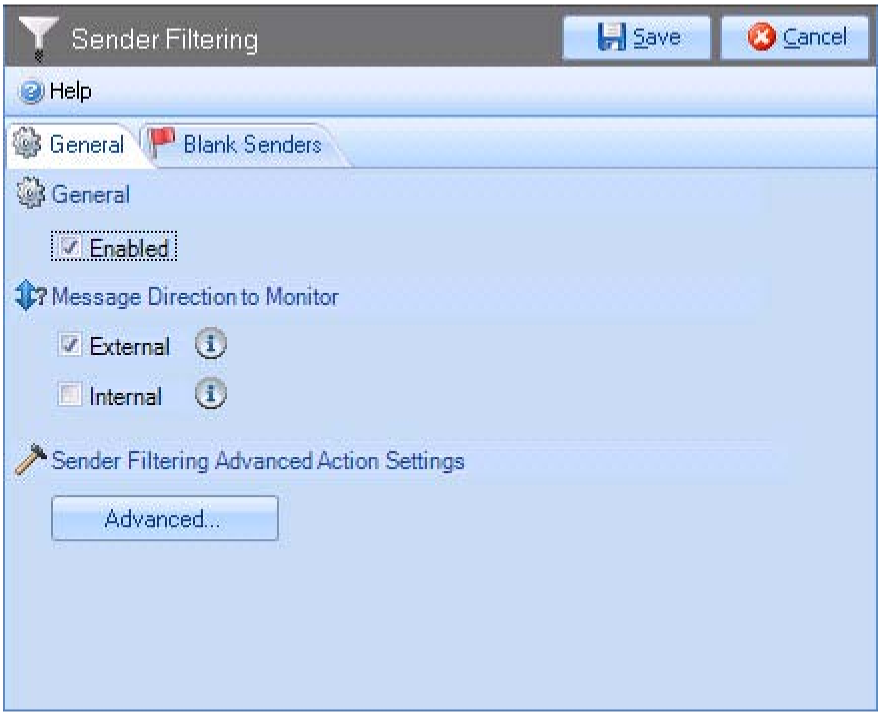
Sender Filtering

Within Exclaimer Anti-spam, you can use the sender block list rule [pg.67] to maintain a list of email addresses and/or email domains which are known to send spam email messages. Having added names to this list, you can specify what action should be taken [pg.69] with email messages received from these senders, and what should happen after these actions have been taken.

The sender filtering feature is used to define the first level of sender blocking. Here, you can choose whether sender filtering is active [pg.158] and whether you wish to block messages from blank senders [pg.160]. You can also use advanced options [pg.159] to determine what should happen with messages received from senders who appear in the sender block list [pg.67].

General

General options are used to define basic settings for the recipient filtering feature:



General

☑ Enabled

Message Direction to Monitor

☑ External

□ Internal

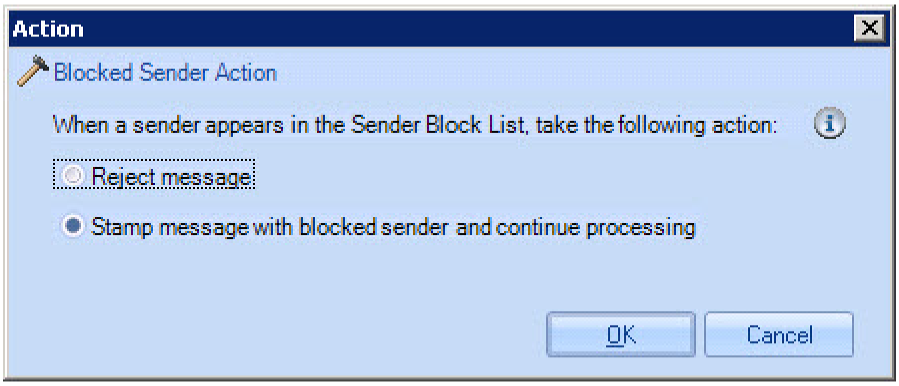
Sender Filtering Advanced Action Settings

These settings are summarized below:

Option	Summary
Enabled	To enable the sender filtering feature, ensure that the enabled check box is ticked.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Advanced Options

You can use advanced options to determine what should happen with messages received from senders who appear in the sender block list:



When a sender appears in the Sender Block List, take the following action:

○ Reject message

● Stamp message with blocked sender and continue processing

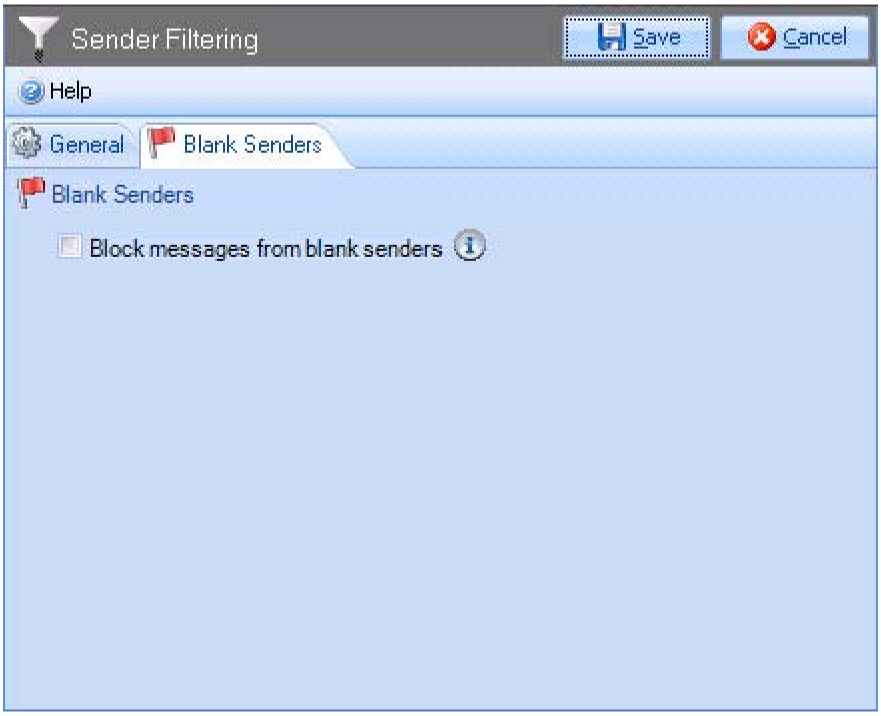
These settings are summarized below:

Option	Summary
Reject message	Select this option to reject the message without any further action.
Stamp message with blocked sender and continue processing	Select this option to highlight the message as being from a blocked sender but then let it continue being processed through the chain of features and then rules [pg.63] before confirming its spam status.

Remember that **features** are processed before **rules**. The sender block list rule [pg.67] includes a range of options to determine what happens to messages received from blocked senders (reject, quarantine, modify, etc) therefore there is no need to reject messages at this stage unless you have a particular reason for doing so.

Blank Senders

The blank senders tab is used to define whether any messages which are received without any sender information should be blocked:



□ Block messages from blank senders

To enable this option, ensure that the check box is selected. If you do not select this option, messages from blank senders will continue through the anti-spam chain of features [pg.120] and rules [pg.63].

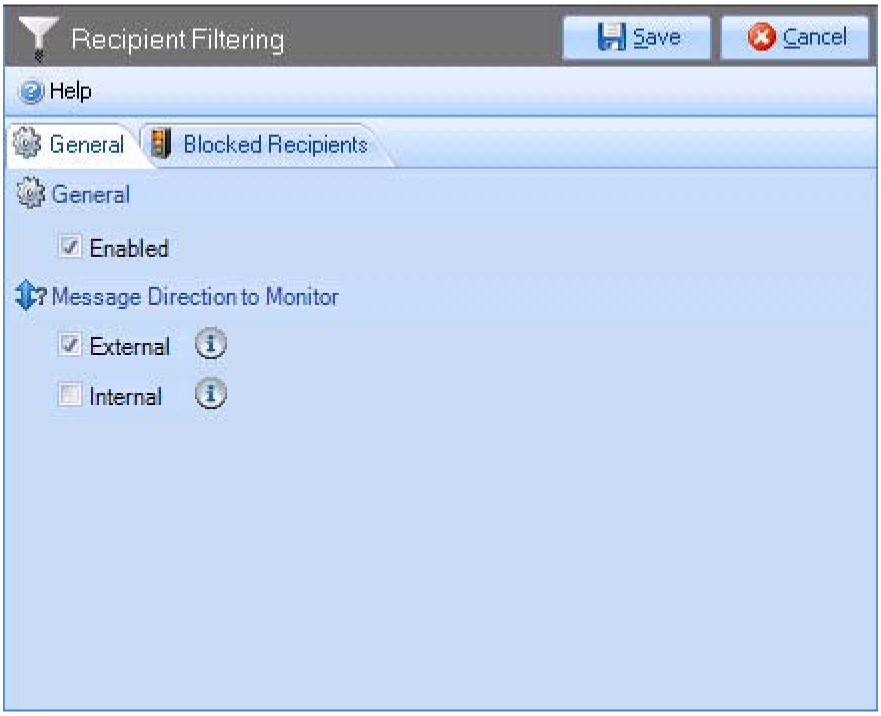
Recipient Filtering

The recipient filtering feature allows you to specify recipients for whom email messages will not be accepted. Here, you can choose whether recipient filtering is active, and whether you wish to block messages that have been sent to recipients who are not listed in the Exchange Global Address List (GAL). The Exchange Global Address List (GAL) stores user information, distribution lists and email addresses and acts as your company's shared email address book.

Use the general tab to update basic settings and the blocked recipients tab to determine Exchange Global Address List (GAL) settings.

General

General options are used to define basic settings for the recipient filtering feature:



General

☑ Enabled

Message Direction to Monitor

☑ External

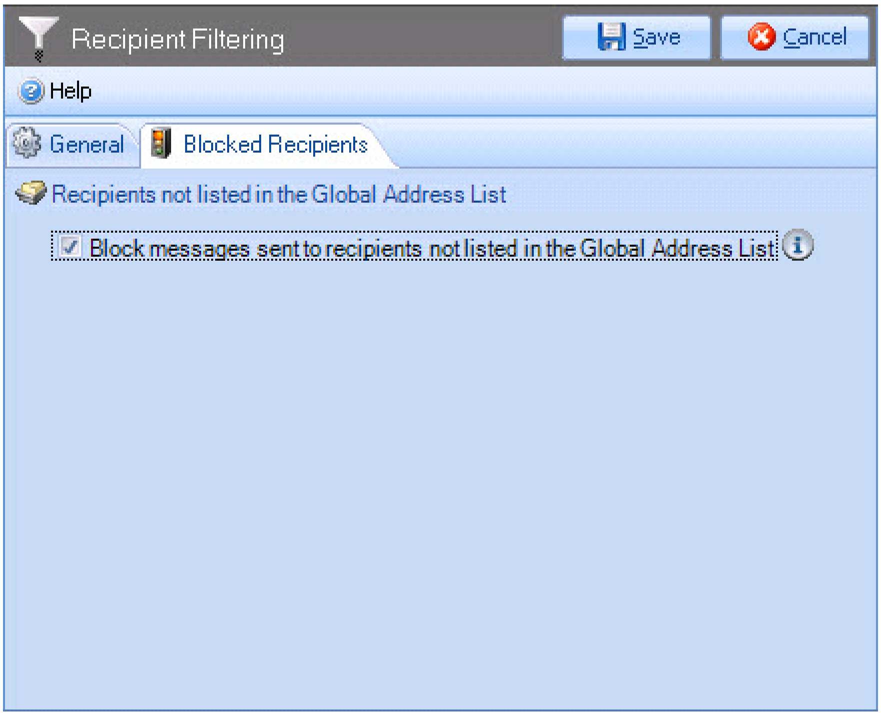
□ Internal

These settings are summarized below:

Option	Summary
Enabled	To enable the recipient filtering feature, ensure that the enabled check box is ticked. If this option is not enabled, both the recipient filtering feature and the recipient white list rule [pg.84] will be disabled.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Blocked Recipients

The blocked recipients tab is used to define whether any messages which are not sent to recipients in the Exchange Global Address List (GAL) should be blocked.



☑ Block messages sent to recipients not listed in the Global Address List

To enable this option, ensure that the check box is selected. If you do not select this option, messages received for recipients who are not in the Exchange Global Address List (GAL) will continue through the anti-spam chain of features [pg.120] and rules [pg.63].

Messages sent from addresses in the **auto white list** will automatically bypass all rules except for **Commtouch classifications** (**Commtouch** checks are performed because they are considered to be extremely accurate). If you have the situation where you need to bypass **Commtouch** checks for an email address, you should add that address to the sender white list [pg.77] and tick the **bypass Commtouch** option.

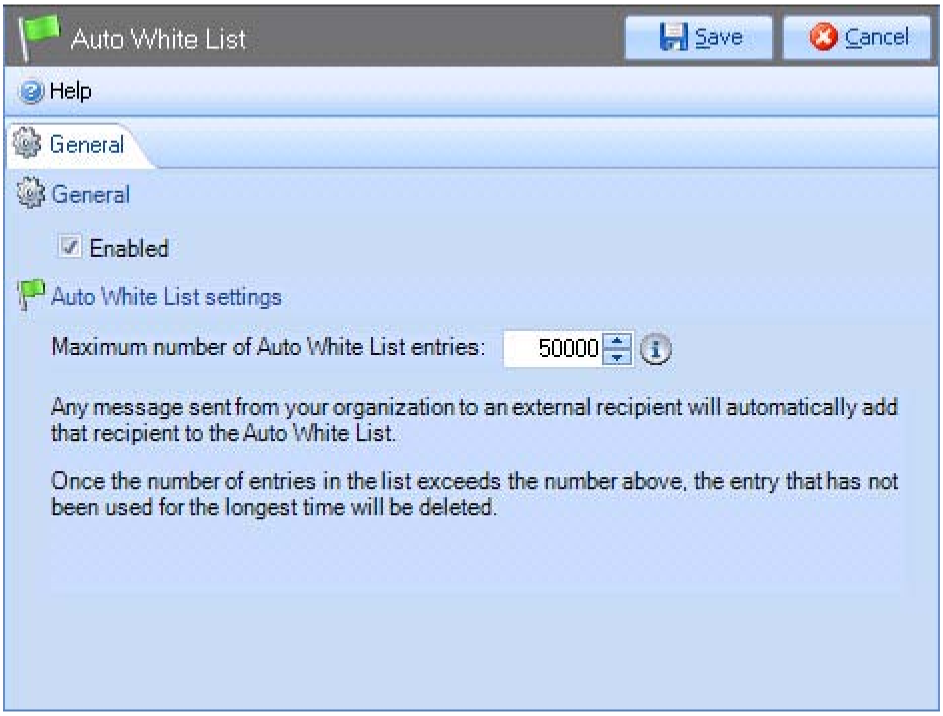
Auto White List

The auto white list feature checks any emails sent from your organization to external recipients and automatically adds those recipients to an auto white list. You can use auto white list options [pg.165] to enable/disable this feature and also to define a maximum number of auto white list entries to be retained.

If you need to remove an entry that has been added to the **auto white list**, you will need to do this outside of the Exclaimer console. If you are unsure how to do this, please refer to the Exclaimer knowledgebase (http://www.exclaimer.com/support-home/KB.aspx).

General

The general tab is used to enable or disable the auto white list feature, and to set a maximum number of auto white list entries:



☑ Enabled

Auto White List settings

Maximum number of Auto White List entries: 50000

Any message sent from your organization to an external recipient will automatically add that recipient to the Auto White List.

Once the number of entries in the list exceeds the number above, the entry that has not been used for the longest time will be deleted.

To enable this feature, ensure that the enabled check box is selected and set the maximum number of auto white list entries is set as required. Once the maximum number of auto white list entries is reached, the entry that has not been used for the longest time will be deleted.

> If you need to remove an entry that has been added to the **auto white list**, you will need to do this outside of the Exclaimer console. If you are unsure how to do this, please refer to the Exclaimer knowledgebase (http://www.exclaimer.com/support-home/KB.aspx).

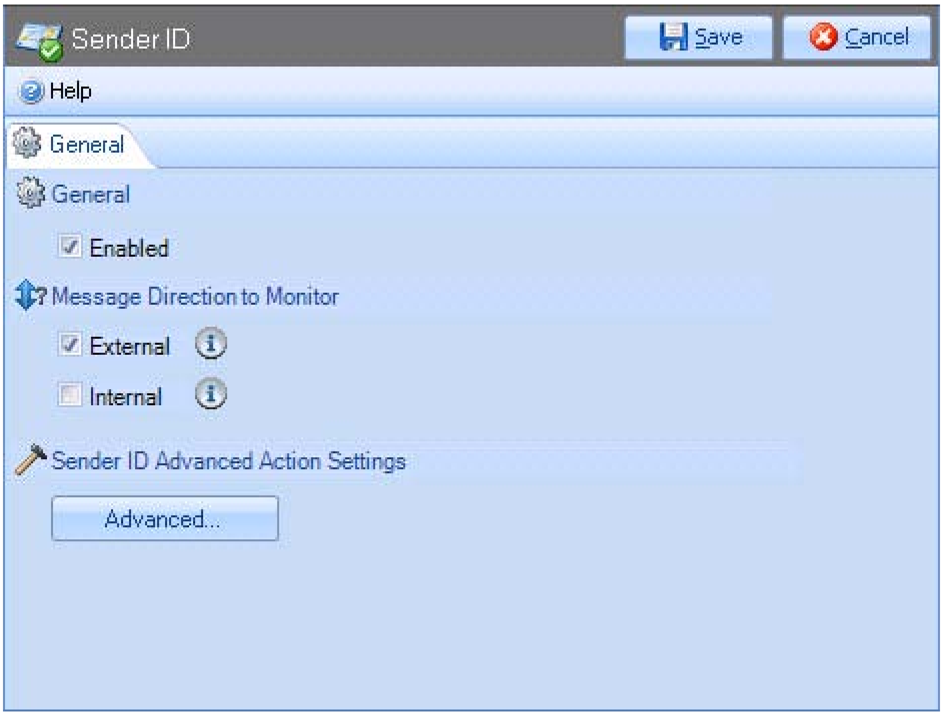
Sender ID

Within Exclaimer Anti-spam, you can use the sender ID rule [pg.89] to check for email spoofing and define what actions should be taken with messages which are stamped with an SPF result of neutral [pg.97], fail [pg.91] or softfail [pg.94] as a result of Sender ID filtering. You can also use general Sender ID settings [pg.90] to determine whether Exclaimer Anti-spam should continue processing rules once Sender ID filtering is complete, or to stop processing rules at this point.

The sender ID feature is used to define the first level of sender ID filtering. Here, you can choose whether sender ID [pg.158] is active. You can also access advanced options [pg.168] to apply a blanket rule as to what action should be taken if sender ID checking identifies that the sender domain is spoofed, and also to specify what should happen if the sender ID checking process should fail for any reason.

General

General options are used to define basic settings for the sender ID feature:



General

☑ Enabled

Message Direction to Monitor

☑ External

□ Internal

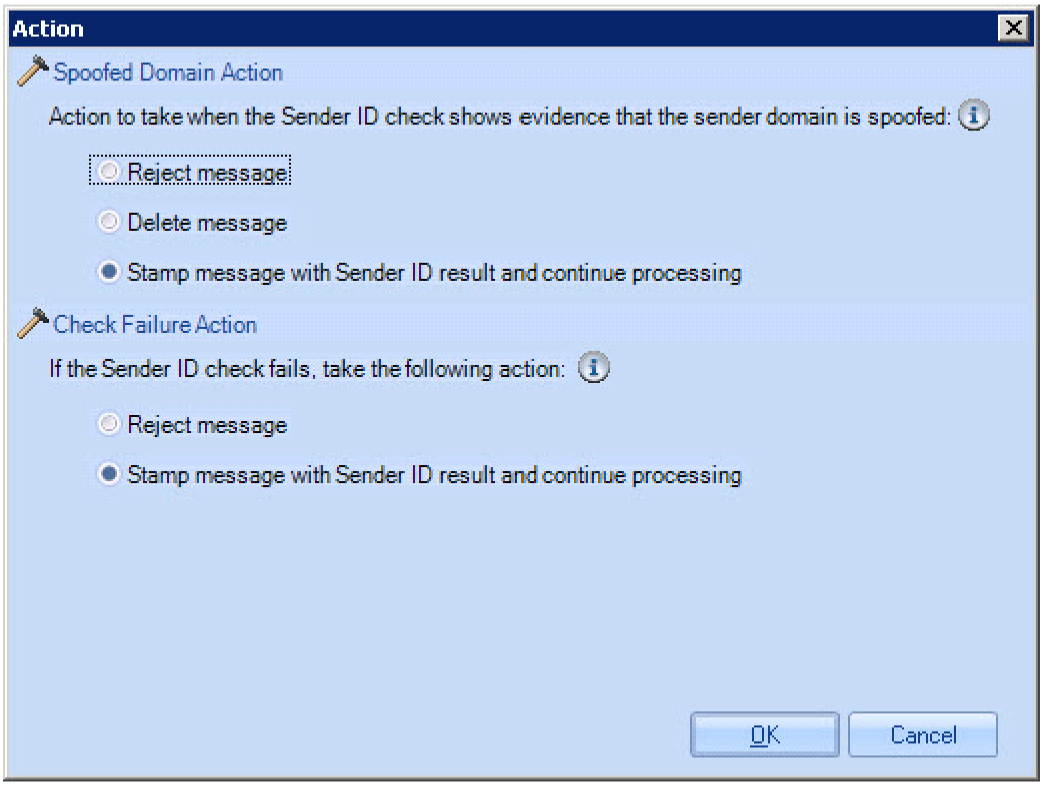
Sender ID Advanced Action Settings

These settings are summarized below:

Option	Summary
Enabled	To enable the sender ID feature, ensure that the enabled check box is ticked. If this option is not enabled, both the sender ID feature and the sender ID rule [pg.89] will be disabled.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

Advanced Options

You can use advanced options to determine what should happen with messages where the sender domain is found to be spoofed, and also to specify what should happen if the sender ID checking process should fail for any reason:



Action

Spoofed Domain Action

Action to take when the Sender ID check shows evidence that the sender domain is spoofed:

○ Reject message

○ Delete message

● Stamp message with Sender ID result and continue processing

Check Failure Action

If the Sender ID check fails, take the following action:

○ Reject message

● Stamp message with Sender ID result and continue processing

These settings are summarized below:

Option	Summary
Action to take when sender ID checks shows evidence that sender domain is spoofed	
Reject message	Select this option to reject the message without further action.
Delete message	Select this option to delete the message. A deleted message is accepted for delivery and then dropped; the recipient does not receive the message and the sender would not receive a message notifying them that delivery failed.
Stamp message with sender ID result and continue processing	Select this option to stamp the message with a sender ID result (neutral [pg.97], fail [pg.91] or softfail [pg.94]) but then let it continue through the chain of features and then rules [pg.63] before confirming its spam status.

Remember that **features** are processed before **rules**. The sender ID rule [pg.89] includes a range of options to determine what happens to messages where the sender domain is found to be spoofed (reject, quarantine, modify, etc) therefore there is no need to reject or delete messages at this stage unless you have a particular reason for doing so.

.../continued

Check failure action	
Reject message	Select this option to reject messages if, for any reason, sender ID checking fails when they are being processed.
Stamp message with sender ID result and continue processing	Select this option to stamp messages and let them continue through the anti-spam chain if, for any reason, sender ID checking fails when they are being processed.

Content Filtering

Content filtering options are drawn from Microsoft's SmartScreen® technology, developed to reduce the amount of spam received by users.

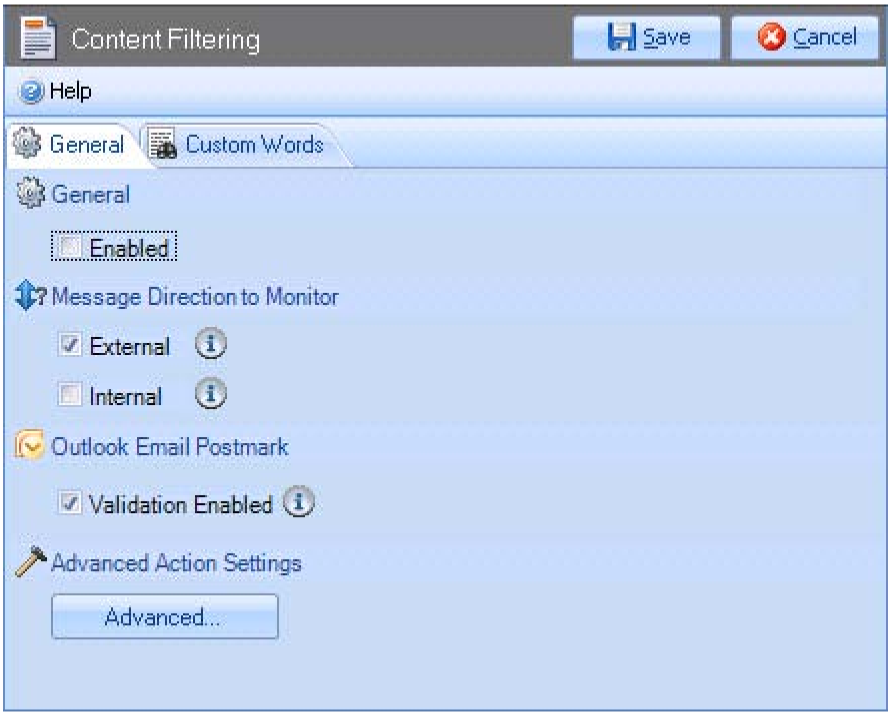
SmartScreen® tracks email characteristics by aggregating user input from hundreds of thousands of Windows Live Hotmail users who subscribed to the voluntary Feedback Loop Program. As such, it can distinguish between legitimate email messages and spam. Additionally, when used with Microsoft Outlook 2010 and Microsoft Exchange 2010, content filtering aggregates your users' Outlook Safe Senders Lists, Blocked Sender List, Safe Recipients Lists and trusted contacts from Outlook.

When email messages are received, textual content is evaluated and a Spam Confidence Level (SCL) rating is assigned and stored as an attribute of the message. An SCL rating is a number between 0 and 9 where 0 indicates that the message is highly unlikely to be spam and a rating of 9 indicates that the message is very likely spam.

The content filtering feature includes two tabs - general [pg.171] and custom words [pg.173]. The general tab is used to define basic settings and also to specify what action should be taken with messages at given SCL thresholds. The custom words tab allows you to maintain a list of allowed / blocked words and phrases for your organization. If you find that certain words are not being identified as spam when they should be, you can add them to a block list and conversely, if you find that certain words are causing messages to be identified as spam erroneously, you can add them to an allow list.

General

General options are used to define basic settings for the content filtering feature. You can also access advanced [pg.172] options to view/update actions to be taken with messages at given SCL thresholds:



Content Filtering

General

□ Enabled

Message Direction to Monitor

☑ External

□ Internal

Outlook Email Postmark

☑ Validation Enabled

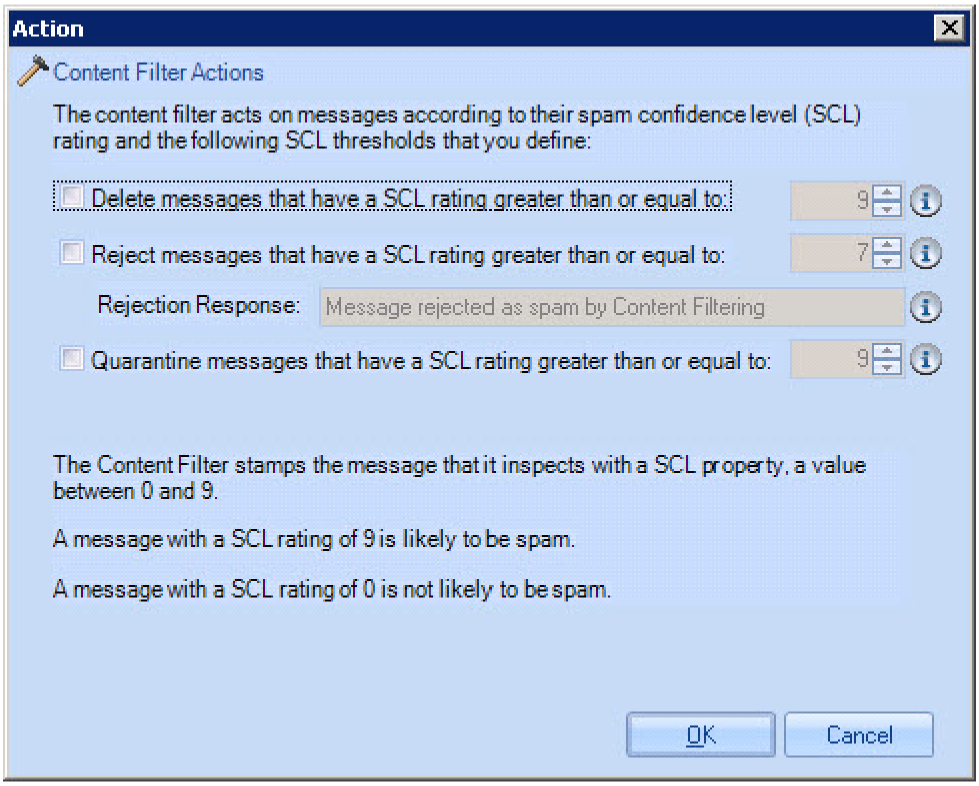
Advanced Action Settings

Basic settings are summarized below (see page 172 for advanced options):

Option	Summary
Enabled	To enable content filtering, ensure that the enabled check box is ticked. If this option is not enabled, both the content filtering feature and the content filtering rule [pg.100] will be disabled.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.
Outlook email postmark	Outlook Email Postmarking (OEP) was introduced in Office Outlook 2007. When an email is sent, it is stamped with an email postmark which incorporates unique characteristics of the message (including recipient details and the time the message was sent). As a result, the postmark is valid only for that email message. When a recipient email application (that supports OEP) receives a postmarked message, it recognizes the postmark and so the message is less likely to be classified as spam. Select the validation enabled option if you wish to validate Outlook email postmarks.

Advanced Options

Advanced options are used to define what action should be taken with messages at different Spam Confidence Level (SCL) thresholds:



The content filter acts on messages according to their spam confidence level (SCL) rating and the following SCL thresholds that you define:

☐ Delete messages that have a SCL rating greater than or equal to: 9

☐ Reject messages that have a SCL rating greater than or equal to: 7

Rejection Response: Message rejected as spam by Content Filtering

☐ Quarantine messages that have a SCL rating greater than or equal to: 9

The Content Filter stamps the message that it inspects with a SCL property, a value between 0 and 9.

A message with a SCL rating of 9 is likely to be spam.

A message with a SCL rating of 0 is not likely to be spam.

These options are summarized below:

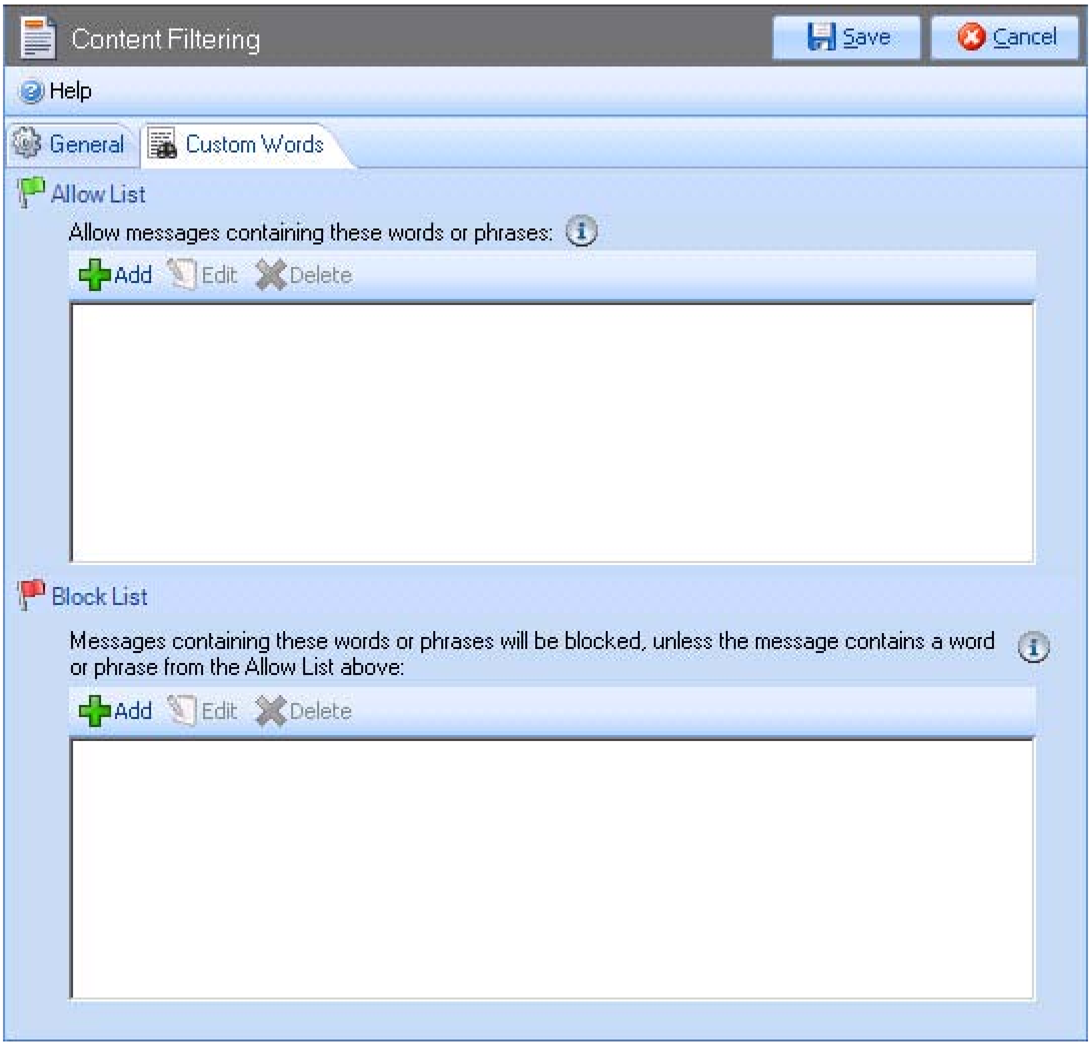
Option	Summary
Delete messages that have a SCL rating greater than or equal to...	When this option is selected, any messages with a Spam Confidence Level (SCL) greater than or equal to your specified value will be deleted. A deleted message is accepted for delivery and then dropped; the recipient does not receive the message and the sender would not receive a message notifying them that delivery failed.
Reject messages that have a SCL rating greater than or equal to...	When this option is selected, any messages with a Spam Confidence Level (SCL) greater than or equal to your specified value will be rejected and a rejection message is sent to the sender.
Quarantine messages that have a SCL rating greater than or equal to...	Select this option to redirect email messages to a predefined Quarantine Mailbox. The Quarantine Mailbox is defined on the Exclaimer Anti-spam options tab [pg.58].

Care should be taken if you are adjusting Spam Confidence Level (SCL) thresholds. A message with an SCL rating of 0 is unlikely to be spam whereas a message with a SCL rating of 9 is very likely to be spam.

Custom Words

The custom words tab is used to maintain an allow list and a block list for your organization.

The allow list is used to add words which are considered to be 'safe' within your organization and the block list is used to define words which are considered to be offensive:



Allow messages containing these words or phrases:

Messages containing these words or phrases will be blocked, unless the message contains a word or phrase from the Allow List above:

When content filtering takes place, messages are checked to see if any allowed/blocked words are present (message body and subject content is checked). If a message contains a word which is included in the allow list, the Spam Confidence Level (SCL) rating will be set to zero irrespective of any rating that was set previously.

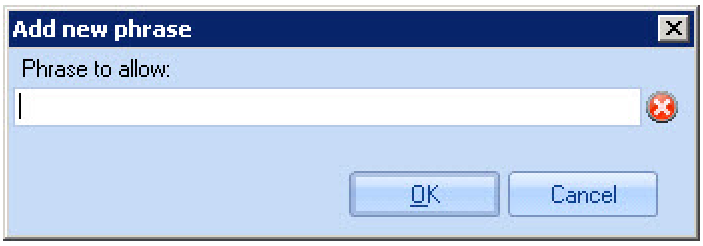
If a message contains a word that is included in the block list, it will be rejected. The only time that a message containing a blocked word would **not** be rejected is where the message also contains a word in the allow list.

Words and phrases are organized in alphabetical order. From here, you can add [pg.174], edit [pg.175] and delete [pg.176] words or phrases as required.

Adding Custom Words

To add a new custom word or phrase, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the content filtering branch.
3. Select the custom words tab.
4. If you wish to update the allow list, move to the upper pane. If you wish to update the block list, move to the lower pane.
5. Click the add button to open the add new phrase window:

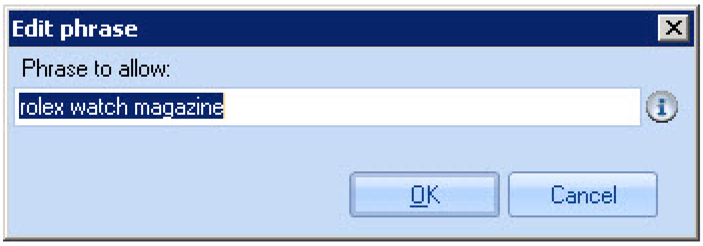


6. Enter the required word or phrase.
7. Click OK to add the entry to the list and exit back to the custom words tab.
8. Add further words and phrases as required.
9. Click the save button (at the top of the window) to save changes.

Editing Custom Words

To edit an existing custom word or phrase, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the content filtering branch.
3. Select the custom words tab.
4. If you wish to update the allow list, move to the upper pane. If you wish to update the block list, move to the lower pane.
5. Select the required word or phrase.
6. Click the edit button to open the edit phrase window:



Edit phrase

Phrase to allow: rolex watch magazine

7. Make changes as required.
8. Click OK to update the entry and exit back to the custom words tab.
9. Click the save button (at the top of the window) to save changes.

Deleting Custom Words

To delete an existing custom word or phrase, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the content filtering branch.
3. Select the custom words tab.
4. If you wish to update the allow list, move to the upper pane. If you wish to update the block list, move to the lower pane.
5. Select the required word or phrase.
6. Click the delete button. You are asked if you are sure that you wish to remove the selected entry.
7. If you are satisfied that the correct word or phrase has been selected, click yes to complete the deletion and exit back to the custom words tab.
8. Click the save button (at the top of the window) to save changes.

If required, you can delete a range of entries at the same time. To select a range of entries that are organised contiguously, press and hold down the **SHIFT** key and then select the first and last entries to be removed. All items between (and including) these points will be selected.

To select a range of entries that are not organised contiguously, press and hold down the **CTRL** key and then select required entries.

Sender Reputation

Sender reputation filtering works by checking a range of known characteristics about the sender in order to calculate a Sender Reputation Level (SRL). In other words, to determine the likelihood of their messages being spam. These checks include:

- HELO/EHLO statement
- Reverse Domain Name System (DNS) lookup
- Analysis of Spam Confidence Level (SCL) ratings on messages from a particular sender (see content filtering [pg.100] for further information about SCL ratings)

The Sender Reputation Level (SRL) is a number between 0 and 9 and it is used to define a threshold for blocking senders. A value of 0 indicates that the sender is not likely to be a spammer whilst a value of 9 indicates that the sender is very likely to be a spammer.

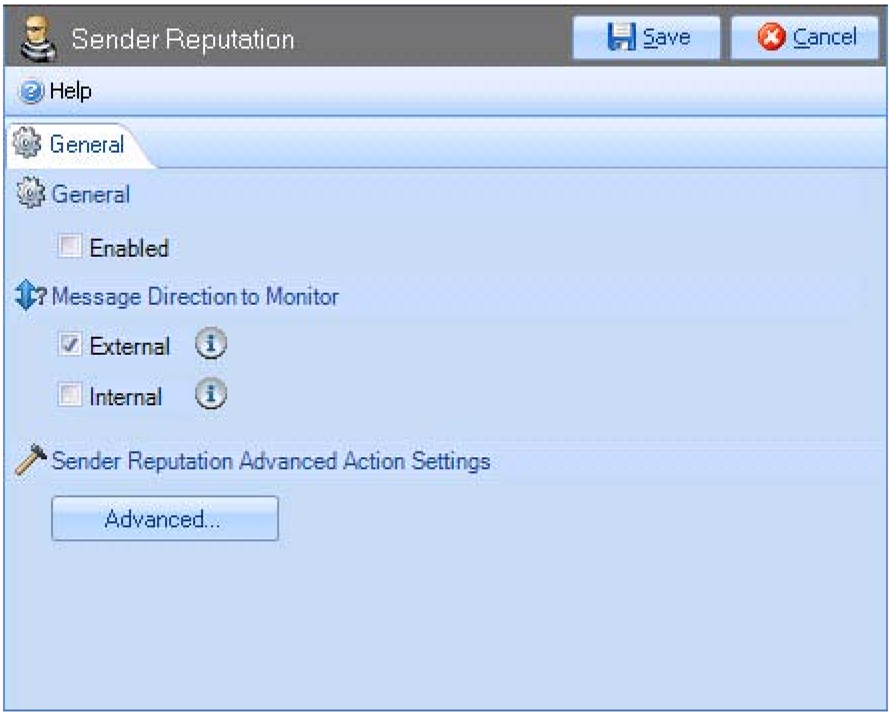
Within Exclaimer Anti-spam, you can set this threshold using sender reputation advanced options [pg.180]. If the threshold is exceeded for a particular sender, the sender reputation filter adds that sender to the IP Block list. You can also use Exclaimer Anti-spam's sender reputation advanced options [pg.179] to set the length of time that the sender remains in the IP block list.

The sender reputation filter also performs an open proxy test. An open proxy is a proxy server that is configured so that anyone can use it. There are public access proxy servers on the Internet that are intentionally open to the public and there are numerous private proxy servers that are left open unintentionally because they are not configured properly. Open proxy servers are often used by spammers because the proxy hides the spammer's own IP address from recipients. Within Exclaimer Anti-spam, open proxy test settings can be defined using sender reputation advanced options [pg.179].

Detailed information about **sender reputation** filtering (including each of these checks) can be found on the Microsoft Technet website (http://technet.microsoft.com/en-us/library/bb124512.aspx).

General

General options are used to define basic settings for the sender reputation feature:



Sender Reputation

General

☐ Enabled

Message Direction to Monitor

☑ External

☐ Internal

Sender Reputation Advanced Action Settings

These settings are summarized below:

Option	Summary
Enabled	To enable the sender reputation feature, ensure that the enabled check box is ticked.
Message direction to monitor	Choose whether to monitor messages received from external parties and/or internal parties.

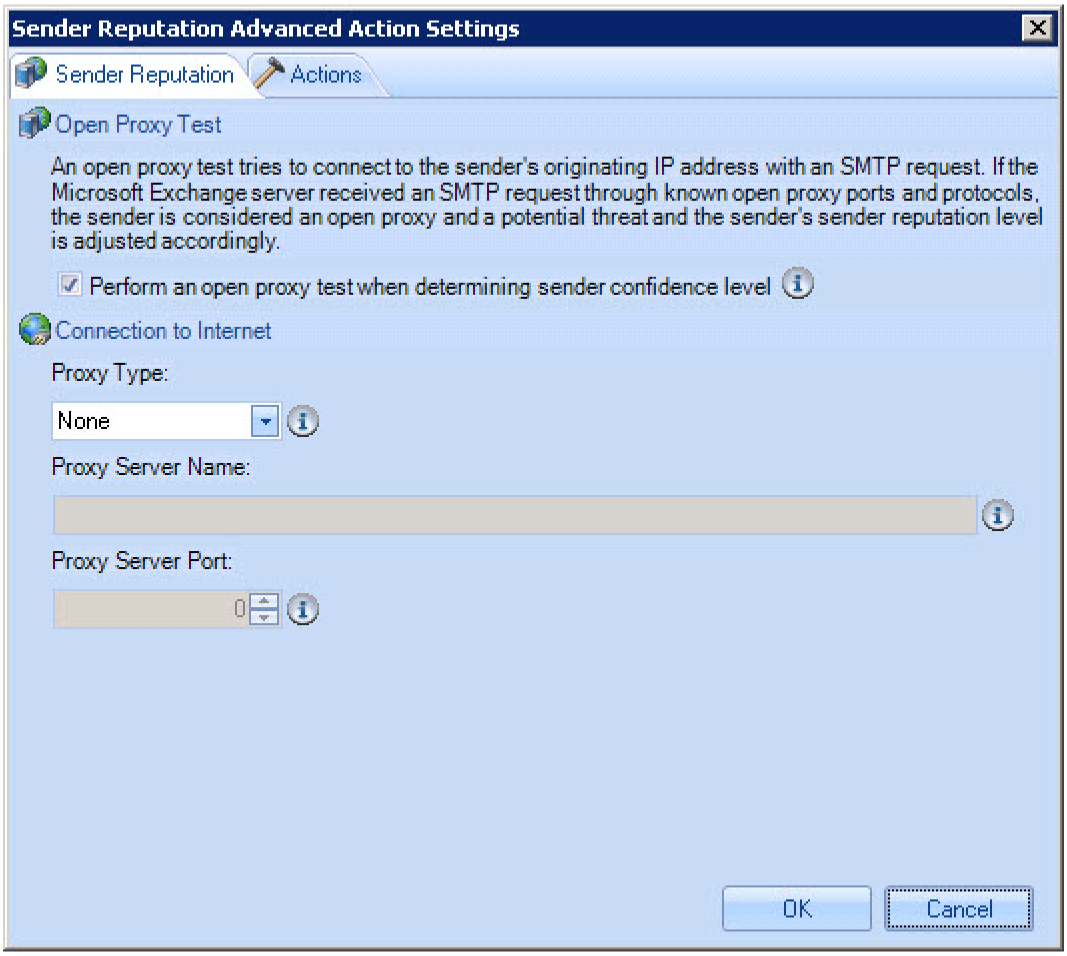
To access settings for open proxy tests and your Sender Reputation Level (SRL) threshold, see advanced options [pg.179].

Advanced Options

You can use advanced options to access settings for open proxy tests and your Sender Reputation Level (SRL) [pg.180] threshold.

Sender Reputation

The sender reputation tab is used to enable or disable open proxy tests:



Sender Reputation Advanced Action Settings

Open Proxy Test

An open proxy test tries to connect to the sender's originating IP address with an SMTP request. If the Microsoft Exchange server received an SMTP request through known open proxy ports and protocols, the sender is considered an open proxy and a potential threat and the sender's sender reputation level is adjusted accordingly.

☑ Perform an open proxy test when determining sender confidence level

Connection to Internet

Proxy Type: None

Proxy Server Name:

Proxy Server Port: 0

Open proxy tests are used to determine if a message has been sent via an open relay (i.e. a proxy server that allows anyone to send email through it). It is very common for spammers to use open relays for sending messages, therefore you can choose to test for open proxies when determining the Spam Confidence Level (SCL) for messages.

In very simple terms, an open proxy test is where the system receives a message and then accesses the Internet to try sending an email through the message sender in a number of different ways.

To enable open proxy testing, ensure that this check box is selected.

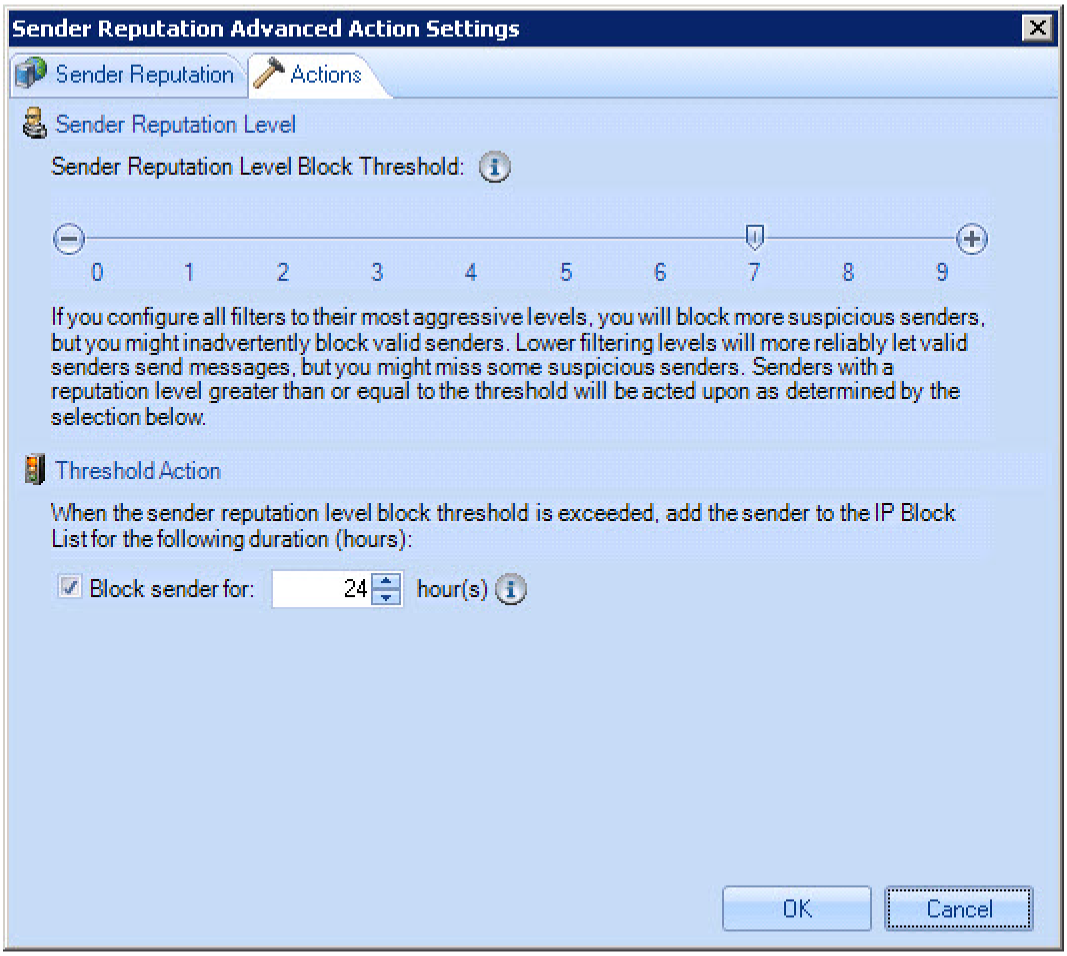
Connection to the Internet

If your Microsoft Exchange server connects to the Internet directly, these options are not required.

Within some organizations the Microsoft Exchange server does not connect to the Internet directly and so needs to go through a proxy server. Having defined a proxy server, the Exchange Server can then connect to the Internet and try all common proxy protocols for open proxy testing. If a Microsoft Exchange server cannot connect to the Internet, open proxy tests cannot be performed.

Actions

The actions tab is used to define a Sender Reputation Level (SRL) threshold for blocking senders. It is also used to set the length of time that blocked senders (i.e. senders who are blocked as a result of sender reputation filtering) remain in the IP block list [pg.132]:



Sender Reputation Advanced Action Settings

Sender Reputation Level

Sender Reputation Level Block Threshold: 7

If you configure all filters to their most aggressive levels, you will block more suspicious senders, but you might inadvertently block valid senders. Lower filtering levels will more reliably let valid senders send messages, but you might miss some suspicious senders. Senders with a reputation level greater than or equal to the threshold will be acted upon as determined by the selection below.

Threshold Action

When the sender reputation level block threshold is exceeded, add the sender to the IP Block List for the following duration (hours):

☑ Block sender for: 24 hour(s)

These options are summarized on the following page.

Sender reputation actions are summarized below:

Option	Summary
Sender reputation level	The Sender Reputation Level (SRL) is a number between 0 and 9 and it is used to define a threshold for blocking senders. A value of 0 indicates that the sender is not likely to be a spammer whilst a value of 9 indicates that the sender is very likely to be a spammer. Use the slider to set the required threshold which, when met or exceeded, triggers the sender to be added to the IP block list [pg.132] for a duration that is configured below.
Threshold action	When sender reputation filtering causes a sender to be added to the IP block list [pg.132], you can configure how long it should remain there (the default duration is 24 hours). After this time, the sender is removed from the block list and can send messages again. If this action is not enabled, senders will not be added to the IP block list. If you wish to add senders with a poor reputation to the **IP block list** for an indefinite period you should manually add them to the IP block list [pg.132] via the blocked addresses tab [pg.134].

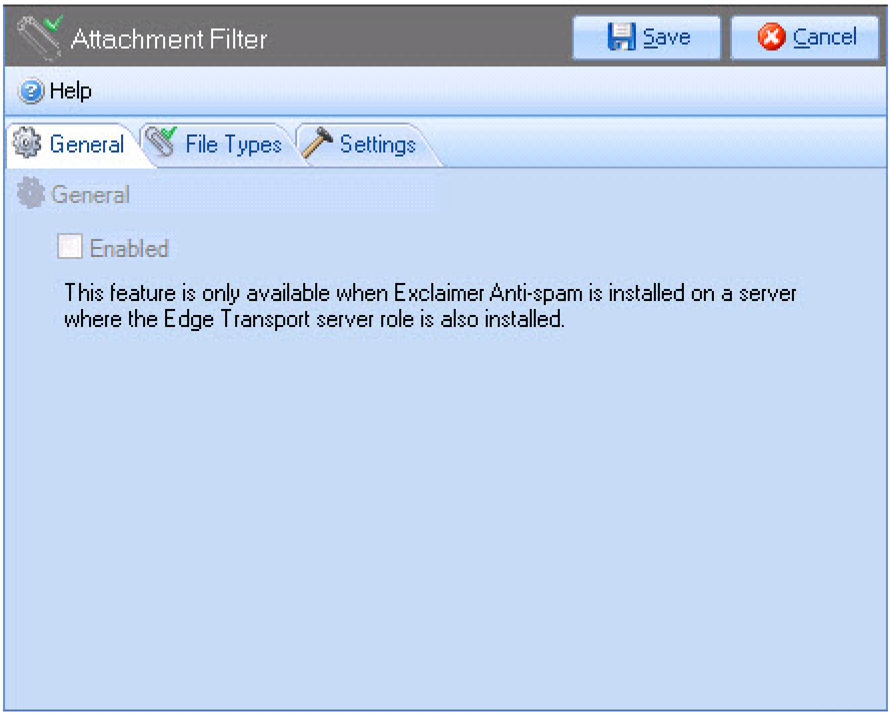
Attachment Filter

When the attachment filtering feature is enabled [pg.182], you can define actions [pg.190] to be taken with email messages containing attachments of a given file [pg.184] or content [pg.187] type.

The **attachment filtering** feature is only available when **Exclaimer Anti-spam** is installed on a server where the **Edge Transport server** role is also installed (for further information about **Edge** and **Hub** transport server roles please see the installation types [pg.14] section).

General

General options are simply used to enable or disable attachment filtering:



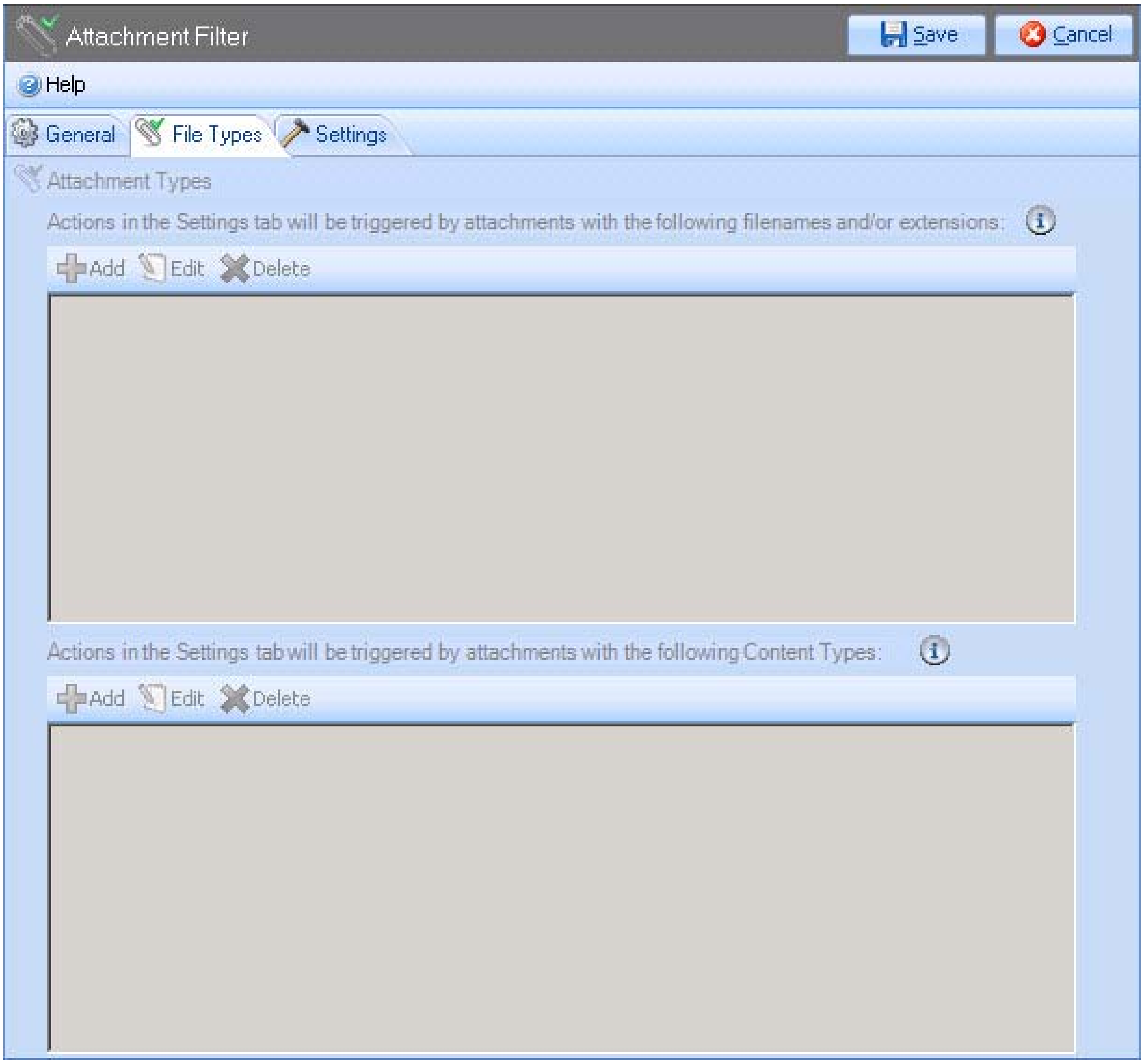
□ Enabled

This feature is only available when Exclaimer Anti-spam is installed on a server where the Edge Transport server role is also installed.

To enable attachment filtering, ensure that the enabled check box is ticked.

File Types

The file types tab is used to define any file [pg.184] and content [pg.187] type that should trigger actions defined on the attachment filtering settings [pg.190] tab. Here, you should add any file or content types which are considered to be offensive or threatening:



Actions in the Settings tab will be triggered by attachments with the following filenames and/or extensions:

Actions in the Settings tab will be triggered by attachments with the following Content Types:

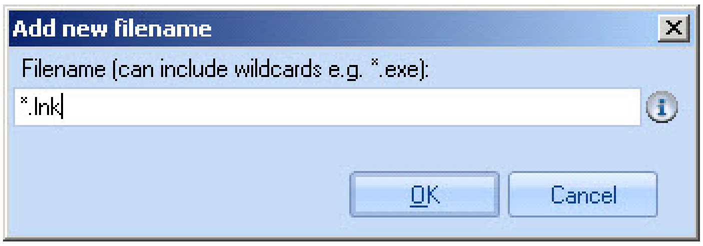
The file types window is split into upper and lower sections; the upper section is used to add [pg.184], edit [pg.185] and delete [pg.186] file types and the lower section is used to add [pg.187], edit [pg.188] and delete [pg.189] content types.

Adding File Types

When adding file types, you can add both file types and file names. For example, you might want to block all attachments which contain an executable program file (an .exe file) and you might also want to block any type of file which contains the word 'warez'.

To add a new file type for attachment filtering, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the attachment filtering branch.
3. Select the file types tab.
4. In the upper section, click the add button to open the add new filename window:



Filename (can include wildcards e.g. *.exe):

*.lnk

5. Enter the required file type using wildcards where appropriate.

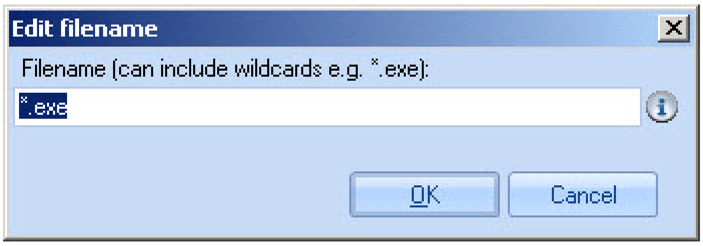
> Wildcards can be used wherever required. For example, to block a specific file type you would prefix that type with ***.** - e.g. ***.exe**. To block any files (irrespective of type) which start with the word 'warez' you would enter **warez*.***

6. Click OK to add the entry to the list and exit back to the file types tab.
7. Add further file types as required.
8. Click the save button (at the top of the window) to save changes.

Editing File Types

To edit an existing file type, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the attachment filtering branch.
3. Select the file types tab.
4. In the upper section, select the file type that you wish to update.
5. Click the edit button to open the edit filename window:



Edit filename

Filename (can include wildcards e.g. *.exe):

*.exe

6. Change the selected file type as required.

> Wildcards can be used wherever required. For example, to block a specific file type you would prefix that type with ***.** - e.g. ***.exe**. To block any files (irrespective of type) which start with the word 'warez' you would enter **warez*.***

7. Click OK to update the entry and exit back to the file types tab.
8. Click the save button (at the top of the window) to save changes.

Deleting File Types

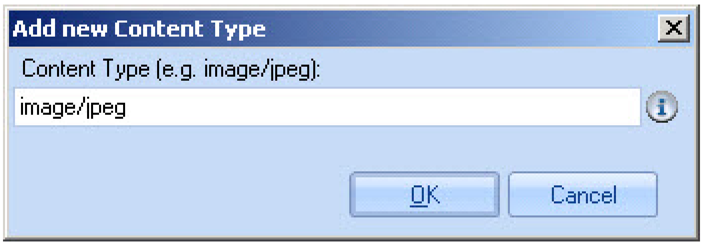
To delete an existing file type, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the attachment filtering branch.
3. Select the file types tab.
4. In the upper section, select the file type that you wish to remove.
5. Click the delete button. You are asked if you are sure that you wish to remove the selected file type.
6. If you are satisfied that the correct file type has been selected, click yes to complete the deletion and exit back to the file types tab.
7. Click the save button (at the top of the window) to save changes.

Adding Content Types

To add a new content type for attachment filtering, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the attachment filtering branch.
3. Select the file types tab.
4. In the lower section, click the add button to open the add new content type window:



5. Enter the required content type. The full MIME content type is required (e.g. image/jpeg). For a list of common MIME types see the Microsoft website (http://technet.microsoft.com/en-us/library/bb742440.aspx).
6. Click OK to add the entry to the list and exit back to the file types tab.
7. Add further content types as required.
8. Click the save button (at the top of the window) to save changes.

Editing Content Types

To edit an existing content type, follow the steps below:

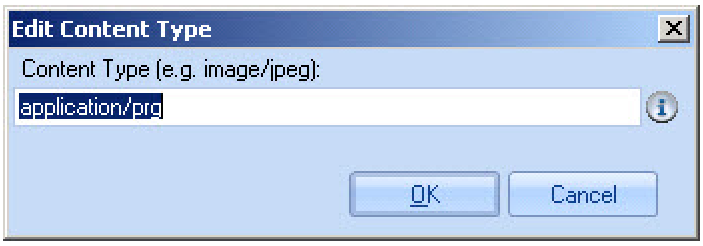
1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].

2. Select the attachment filtering branch.

3. Select the file types tab.

4. In the lower section, select the content type that you wish to update.

5. Click the edit button to open the edit content type window:



Edit Content Type

Content Type (e.g. image/jpeg): application/prg

6. Change the selected content type as required. The full MIME content type is required (e.g. image/jpeg). For a list of common MIME types see the Microsoft website (http://technet.microsoft.com/en-us/library/bb742440.aspx).

7. Click OK to update the entry and exit back to the file types tab.

8. Click the save button (at the top of the window) to save changes.

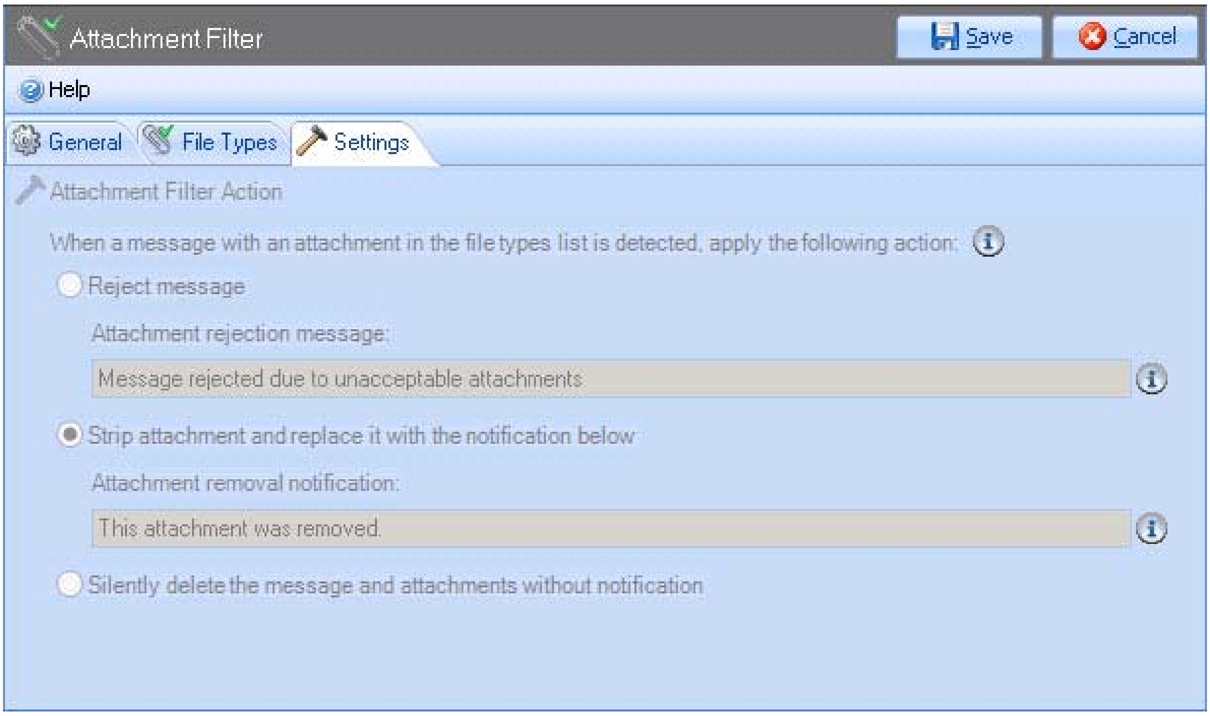
Deleting Content Types

To delete an existing content type, follow the steps below:

1. Expand the Anti-spam features branch of the Exclaimer console tree [pg.34].
2. Select the attachment filtering branch.
3. Select the file types tab.
4. In the lower section, select the content type that you wish to remove.
5. Click the delete button. You are asked if you are sure that you wish to remove the selected file type.
6. If you are satisfied that the correct content type has been selected, click yes to complete the deletion and exit back to the file types tab.
7. Click the save button (at the top of the window) to save changes.

Settings

The settings tab is used to specify what action should be taken when defined file or content types [pg.183] are detected in email attachments:



Attachment Filter Action

When a message with an attachment in the file types list is detected, apply the following action:

○ Reject message

Attachment rejection message:

Message rejected due to unacceptable attachments

● Strip attachment and replace it with the notification below

Attachment removal notification:

This attachment was removed.

○ Silently delete the message and attachments without notification

These options are summarized below:

Option	Summary
Reject message	Select this option to reject email messages which are associated with a blocked attachment type. Use the attachment rejection message field to advise the sender that their message has been rejected due to the nature of its attachment(s).
Strip attachment and replace it with the notification below	Select this option to remove the attachment and use the attachment removal notification field to advise recipient(s) that the original message contained an attachment which has been removed. Remember that this is only one check. The email message could still be rejected if subsequent features or rules identify it as spam.
Silently delete the message and attachments without notification	Select this option to delete the attachment and also the message without sending any form of notification to either sender or recipient(s).

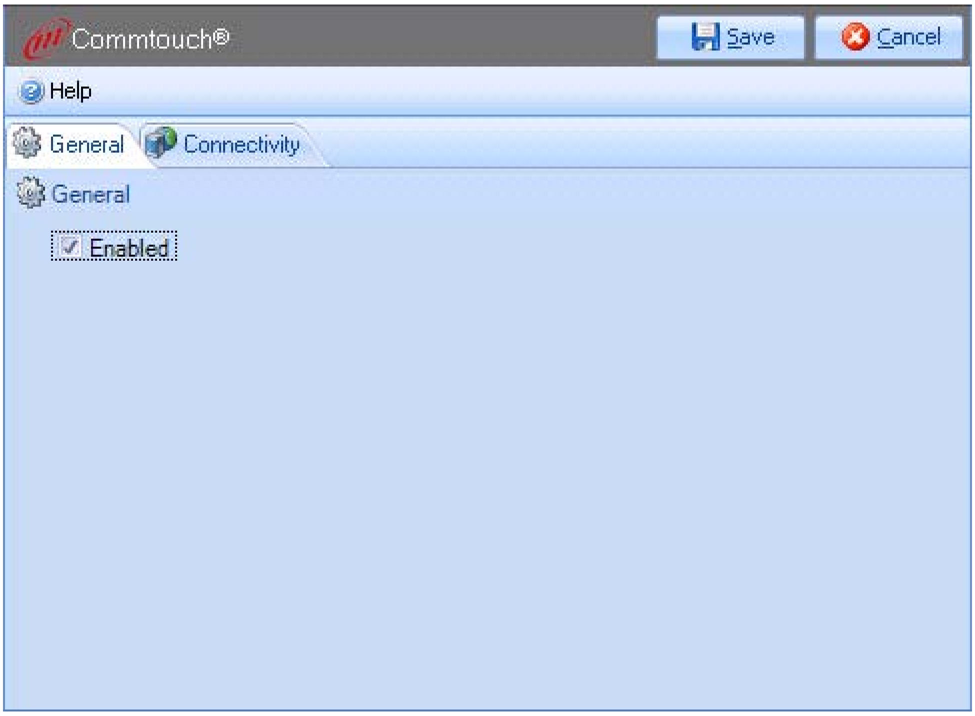
Commtouch

Exclaimer Anti-spam has integrated the Commtouch anti-spam solution to offer an additional layer of security (for further information about Commtouch, please see the Commtouch classifications [pg.106] section of this guide).

The Commtouch feature allows you to enable/disable Commtouch [pg.192] and to define proxy server settings [pg.193] (should you need to access the Internet via a proxy server).

General

General options are used to enable or disable the Commtouch feature:



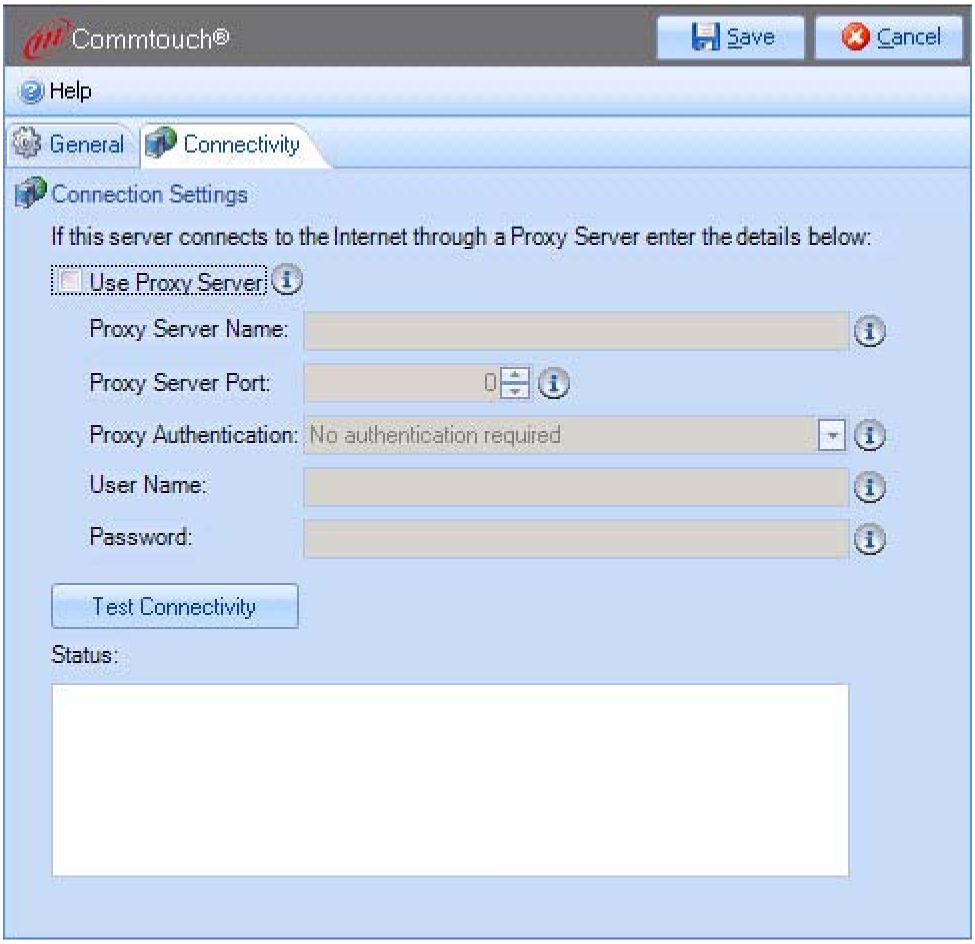
☑ Enabled

To enable Commtouch, ensure that the enabled check box is ticked. You can then use the connectivity [pg.193] tab to view or change connection settings. If this option is not enabled, both the Commtouch feature and the Commtouch classifications rule [pg.106] will be disabled.

Connectivity

Having integrated the Commtouch solution, Exclaimer Anti-spam interrogates the Commtouch database to obtain classifications for incoming email messages in real time.

If you need to access the Internet through a proxy server, settings must be defined on the connectivity tab:



If this server connects to the Internet through a Proxy Server enter the details below:

☐ Use Proxy Server

Proxy Server Name:

Proxy Server Port: 0

Proxy Authentication: No authentication required

User Name:

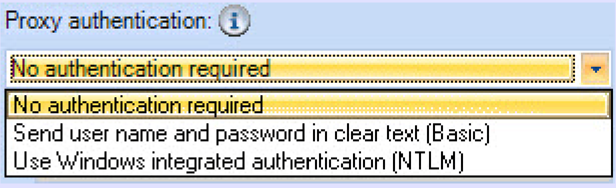
Password:

Status:

These options are summarized on the following page.

Exclaimer Anti-spam requires an Internet connection. If a direct Internet connection is not detected, you must define connectivity settings and use **the test connectivity** button to confirm these settings before you will be able to proceed.

Connectivity options are summarized below:

Option	Summary
Use proxy server	Select this option if you are using a proxy server. Once selected, subsequent options become active.
Proxy server name	Enter the name of your proxy server.
Proxy server port	Use the arrow button associated with this field to select the required port number for the proxy server.
Proxy authentication	Use the drop-down list to determine the type of authentication that is required:  Proxy authentication: No authentication required No authentication required Send user name and password in clear text (Basic) Use Windows integrated authentication (NTLM) Here, you can choose to operate with no authentication, to send username and password in clear text (unencrypted, human-readable data) or to use Windows integrated authentication. If you choose one of the authentication methods (clear text or Windows), you should specify required user credentials as well.
Check	Use the check button to check your Internet options. If you have defined proxy settings, this test will ensure that the settings are correct. If you are not using a proxy server, your Internet connection will still be checked.

Further Help & Support

Exclaimer Support

	Contact Details
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

	Email	Telephone
UK Sales	sales@exclaimer.com	01252 531422
US & Canada Sales	usasales@exclaimer.com	+1-888-450-9631
Benelux Sales	sales@exclaimer.nl	+31 (0) 228-567066
Germany Sales	sales@exclaimer.de	+49 (0) 421 5371 458
South African Sales	sales@exclaimer.co.za	+27 (0) 11 561 0900
Hungary Sales	sales@exclaimer.com	+36 20 422 3984
France Sales	sales@exclaimer.com	+33 4 76 21 17 03
Spain Sales	sales@exclaimer.es	+34 947 257 714
Rest of the World (UK)	sales@exclaimer.com	+44 (0) 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 Anti-spam 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: 13th May 2011

exclaimer™
Don't press send without it!