



**This document provides information to install and use
X-Spam for Microsoft Exchange Server 2000-2003**

**X-Spam for Microsoft Exchange Server 2000-2003
User Guide**

Copy Right Notice

User Guide of X-Spam for Microsoft Exchange Server 2000-2003

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Document Number : XSMES/25.6.04

Copyright Notice

Copyright (C) 2004. All rights Reserved.

Portions (C) by Kaspersky Labs International Limited.

Any technical documentation that is made available by MicroWorld is the copyrighted work of MicroWorld and is owned by MicroWorld.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and MicroWorld makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of MicroWorld.

Trademarks.

MicroWorld, MicroWorld Logo, eScan, eScan logo, MWL, MailScan are trademarks of MicroWorld.

Windows is a registered trademark of Microsoft Corporation; Kaspersky is a registered trademark of Kaspersky Labs.

All product names referenced herein are trademarks or registered trademarks of their respective companies. MicroWorld Software Services Pvt. Ltd. (MicroWorld) disclaims proprietary interest in the marks and names of others. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. MicroWorld Software Services Pvt. Ltd. reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld Software Services Pvt. Ltd.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical Support: support@mwti.net

Sales: sales@mwti.net

Printed : MicroWorld

June, 2004

Table of Contents

Welcome	5
ABOUT THIS GUIDE	5
AUDIENCE	5
HOW THIS GUIDE IS ORGANIZED	5
TYPOGRAPHICAL CONVENTIONS	6
CONTACT US	7
About MicroWorld	8
ABOUT SPAM	8
ABOUT X-SPAM	8
FEATURES OF X-SPAM	9
X-Spam Tasks	10
TOPICS IN X-SPAM TASKS	10
TO LAUNCH X-SPAM TASKS	10
DETAILS OF X-SPAM TASKS	10
Getting Started	12
USER INTERFACE	12
SCREEN COMPONENTS	12
X-Spam Administrator	14
TOPICS IN X-SPAM	14
ADMIN	15
SMTP CONFIG (GATEWAY CONFIGURATION)	15
SMTP SPAM – GENERAL CONFIGURATION	17
SMTP SETTINGS	18
SMTP CONTROLS	19
SUBSTITUTE DOMAINS	22
MAILS FROM USERS	24
MAILS TO USERS	25
ACKNOWLEDGEMENT & ROUTING BY USERS	26
SMTP SPAM – SPAM CONFIGURATION	27
AUTHENTICATION	27
INTERNET	29
RESTRICTION FROM USERS	30
RESTRICTION TO USERS	31
RBL / DUL SETTINGS	32
SPAM SMTP CONTROLS	34
CONTENT FILTER	34

ACTION	35
STATISTICAL FILTER	36
HEURISTIC FILTER	37
META TEST	39
WHITE / BLACK LIST	41
UPDATE CONFIG	42
SET GENERAL CONFIG	42
FTP CONFIG	44
HTTP CONFIG	47
VIEW	47
VIEW LOG FILE	48
VIEW DOWNLOAD LOG	48
VIEW UPDATE LOG	48
FLUSH LOG	48
MAIL DEBUG INFORMATION	48
REPORT	48
HELP	50
TEST SPAM	50
SPAM HELP	50
LICENSE INFORMATION	50
CHANGE PASSWORD	50
ABOUT	50
Index	51

Welcome

X-Spam for Microsoft Exchange Server 2000-2003 protects your Microsoft Exchange Server against Spam. Spam or junk mail causes losses that run into billions of dollars. This document provides information to install and use X-Spam.

About this Guide

This chapter provides details about the following topics:

- [Audience](#)
- [How this guide is organized](#)
- [Typographical Conventions](#)
- [Contact Us](#)

Audience

This Guide is for system administrators and users involved in installing and using the application.

How this guide is organized

This guide is organized into separate books. The first four books describe basic tasks like getting started, navigation, Installation etc. X-Spam Administrator provides all details to run X-Spam. Each screen and field occurring in the user interface is explained in detail along with the relevant screen shots.

[Overview](#): Provides details of MicroWorld and X-Spam. The section describes the product in brief and also provides a list of X-Spam features.

[Getting Started](#) gives information about a typical screen, its components, types of fields, dialog boxes, tab pages and how to validate them.

[X-Spam Administrator](#): Provides detailed information to run X-Spam. There are three main menus: Admin, View and Help. [Admin](#) includes details to run: Scanner Administration, Content Control, Compression Control, Messages, License Information, Spam Test Mail and Send Debug

Information. [View](#) provides information to: View Log Files, Flush Logs, X-Spam Reports and [Help](#) includes information to Send Spam Test Mail, X-Spam Help, License Information and information to Change Password.

Typographical Conventions

The following typographical conventions are used in this guide.

This	Represents
Bold	A Menu or a menu option. When enclosed in “ “, the name is as displayed in the screen.
“ “	A long name is denoted by the first few words and It is enclosed in ‘ ‘.
SMALL CAPS	Buttons on dialog boxes/child windows.
<i>Italics</i>	Entry Fields in dialog boxes/child windows.
Type	Information you need to enter.
Hyperlink	Is a hyperlink? Click to access related topics.
Tasks	Represents a key task of feature.

- When you have to navigate between menus the following convention is used: menu > menu >...

E.g.. **SMTP Spam Config > General Configuration > SMTP Settings**. Means: in SMTP Spam Config, **select** (click) General Configuration and **choose** (click) SMTP Settings.

Contact Us

We offer 24x7 support to our customers through e-mail, telephone and Chat.

Chat Support

- Chat with our support team at 'escanchat' using: AOL; MSN or Yahoo messenger service.

E-Mail Support

- If you have any queries about our products or have suggestions and comments about this guide, please send them to support@mwti.net

Head Office: MicroWorld Technologies Inc. 33045 Hamilton Court East, Suite 105 Farmington Hills, MI 48334-3385, US. Tel: (248) 848 9081/ 848 9084 Fax: (248) 848 9085	Asia Pacific: MicroWorld Software Services Pvt Ltd.. Plot No 80, Road 15, MIDC, Marol, Andheri (E), Mumbai, INDIA. Tel (91) - 22- 28265701 - 05 Fax (91) - 22-28304750
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

For sales enquiry, e-mail: sales@mwti.net

About MicroWorld

MicroWorld is one of the leading solution providers in the areas of Spam Control, CRM, Content Security and Anti-Virus products for desktops, large corporate networks and MailServers. With its corporate head quarters in New Jersey and development center in Mumbai, India, we offer round-the-clock support, through our regional offices and over 10,000 channel partners spread across the globe. This section provides information about XSpam. Details about its features, how to use it; what to do when you have a virus etc. is given.

About Spam

Spam or unsolicited/junk mail costs us millions of dollars. It is usually sent by companies or individuals of uncertain origin and solicits reader's attention by sending unwanted advertisements or offers using e-mails.

Earlier Spam was a nuisance and all a user had to do was to delete the mail without opening it. But even though the user deletes Spam, it is still delivered by the mail server and valuable bandwidth is lost in storing and relaying it. Nowadays Spam has taken a turn for the worse and could even lead to security issues. Some of the security issues are:

Identity theft. Many e-mail scams are distributed as Spam directly leading to identity theft and fraud.

Viruses. New viruses, worms, and malware, such as Melissa, Love Bug, and MyDoom use Spam techniques to propagate after being triggered by the user.

Combining exploits and Spam. Many Spammers have incorporated malicious code that targets browser, HTML, and Javascript vulnerabilities. For example, on 31-December-2002 a group of hackers in Brazil sent Spam containing a hostile Javascript to millions of users. People that viewed this Spam from Hotmail unknowingly compromised their accounts. It is widely believed that some viruses are designed to assist Spammers. For example, the SoBig worm installed open proxies that were used to relay Spam. As Spam becomes more prevalent, the use of malware and spyware to support Spam is likely to increase.

About X-Spam

X-Spam offers an intelligent solution that allows you to control how Spam is identified. Many legitimate mails from clients and friends may have subject lines like "Hi, long time no see" or "We enjoyed ourselves" and so on. Ordinary Anti Spam software makes a cursory examination of subject lines and because Spam also have these subjects, falsely identifies genuine or friendly mail as Spam and deletes them.

X-Spam on the other hand uses a combination of regular expressions where each instance of suspect Spam is assigned a score. Only when the score reaches a threshold level, signifying the mail has tested positive for multiple Spam tests is the mail identified as Spam.

Features of X-Spam

Key features of X-Spam are:

- Spam is identified and blocked in the mail server itself. Users need not download Spam, open it and then realize that the mail is Spam. This saves valuable bandwidth.
- Allows you to configure your mail server to optimize X-Spam performance.
- Uses Regular Expressions that are sets of rules to identify Spam. These regular expressions can be used singly or in a series. Each has a score associated with it. When mails are tested for Spam, they must test positive for a rule and the score is added to the total. Only when the total reaches a threshold value is the mail identified as Spam.
- X-Spam allows you to create customized rules or regular expressions to refine Spam testing
- The regular expressions can be used in a combination to test mails
- Mails identified as Spam are automatically forwarded to a Spam folder and isolated

X-Spam Tasks


X-Spam has a group of tasks for Spam scanning and blocking. By default, the software is configured to execute them automatically. You can run some of the tasks manually. This section provides a list of different tasks, manually run with X-Spam. Detailed explanations of the tasks, meanings of fields etc are described in successive individual chapters.

Topics in X-Spam Tasks

The chapter provides details about the following topics:

- [To launch X-Spam tasks](#)
- [Details of X-Spam tasks](#)

To launch X-Spam tasks

- After the application is installed, in the application status bar, right click on .
- A drop-down menu is displayed. Tasks are displayed as links. Click on the task to open it.

Details of X-Spam tasks

Details of each item are explained in the following table.

Task Name	Function
Spam Administrator	Opens the X-Spam Administrator Interface that allows you to run X-Spam
Disable Spam Control	Disables or stops X-Spam from running. MicroWorld recommends that you exercise this option with forethought, as your mail server is unguarded when X-Spam is disabled.
Download Spam Updates	Begins auto-download of Spam updates.

Task Name	Function
Send Debug Information	Sends e-mail of bugs and other problems to the system administrator. For more details, refer Send Debug Information .
Send Test Spam Mail	Allows you to send a test Spam mail . If X-Spam is properly installed, then the mail is blocked.
Disable XScan	Disables or stops X-Spam from running. MicroWorld recommends that you exercise this option with forethought, as your mail server is unguarded when X-Spam is disabled.
System Information	Provides information about your system
View Logs	Allows you to view log files that display details of X-Spam activity in your system. For details, refer View Log Files .
About	Displays a splash screen giving information about MicroWorld, the company that makes X-Spam. Version number of the product you are using is also displayed.
Exit	Exits from X-Spam. The software continues to run in the background

Getting Started

This chapter gives details of standard conventions used in this guide. Also included are components of a typical user interface, how to navigate the screens, meanings of various symbols and buttons, types of fields and how to enter values in them.

The following topics are covered in this Chapter:





- User Interface
- Screen Components

User Interface

User interface is the front end of the software. The software is made of different screens. You carry out tasks; enter values, set preferences, etc., using screens. This section explains the components of a typical user interface.

Screen Components

Typical screen components are explained below:

Screen Component	Function
SMTP Spam Config 	Runs the SMTP Spam Config menu. Allows you to configure your SMTP mail server to control Spam
Content Filter 	Runs the Content Filter menu. Allows you to configure X-Spam for effective content control of Spam
SMTP Config 	Runs the SMTP Config menu. Allows you to configure your SMTP mail server
Update Config 	Runs the auto Update Config menu. Allows you to configure your updater to automatically download updates

Screen Component

Function

Arrows

These navigation arrows allow you to scroll up and down the menu frame



Exit

Exits from X-Spam. X-Spam continues to run in the background.



X-Spam Administrator

X-Spam provides a reliable means to protect your system from Spam. The latest threat that we face in the wired world today is Spam or unsolicited junk mail. This section provides information on using X-Spam to block Spam and Spammers.

Topics in X-Spam

The following topics are explained in this section:

Admin

- [SMTP Config \(Gateway Configuration\)](#)
- [SMTP Spam – General Configuration](#)
- [SMTP Spam – Spam Configuration](#)
- [Content Filter](#)
- [Update Config](#)

View

- [View Log File](#)
- [Flush Log](#)
- [Mail Debug Information](#)
- [Report](#)

Help

- [Test Spam](#)
- [Spam Help](#)
- [License Information](#)
- [Change Password](#)
- [About](#)

Admin

The Admin menu contains a set of menus that allow you to configure settings for X-Spam. The next sections explain different menus in detail.

- [SMTP Config \(Gateway Configuration\)](#)
- [SMTP Spam – General Configuration](#)
- [SMTP Spam – Spam Configuration](#)
- [Content Filter](#)
- [Update Config](#)

SMTP Config (Gateway Configuration)

Your SMTP server is the gateway through which users send and receive mails. The screen allows you to configure your MailServer Gateway for both incoming and outgoing mails. You can create a list of local domains, specify their IP and the port used to send and receive mails.

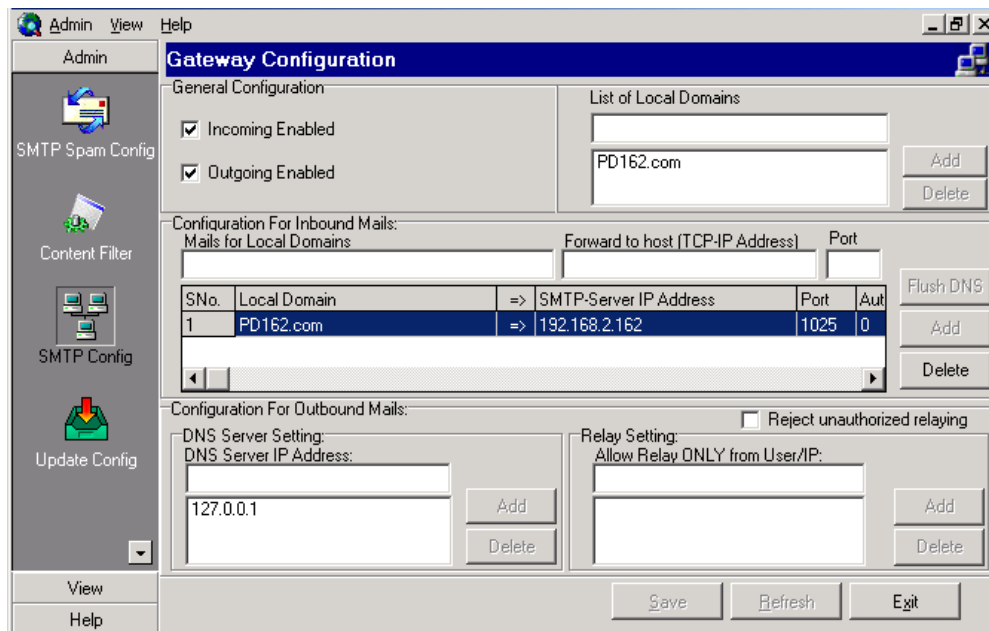


Figure 7.1 Gateway Configuration

Field Name **Description**

General Configuration This frame allows you to specify settings for general configuration.

Incoming Enabled SMTP is allowed to receive mails, if the check box is selected.

Outgoing Enabled SMTP is allowed to send mails, if the check box is selected.

List of Local Domains The frame allows you to specify local domain names for the MailServer.

Enter the local domain name in the top field and select **Add**. The [Edit Local Domain to IP Mapping](#) box is displayed.



Configuration for Inbound Mails: The frame allows you to specify domains, from which mails are allowed to enter your mail server, its IP address and the port number. Mails can be received from local domain.

To Add a local domain:

Click in the fields and enter valid values for 'Mails for Local Domains', 'Forward to host (TCP-IP Address)' and 'Port'. Select **Add** button.

Mails for Local Domains Enter the local domain names, managed by the SMTP Server.

Forward to Host (TCP-IP Address) Enter IP address of Remote SMTP server. Local domains connect to the SMTP server through this IP.

Port Enter port number used to connect to the SMTP server by the local domains.

“Display Box” List box displays local domains names, SMTP server IP address they connect to and the port number. Double click in the list box to view a dialog box that allows you to enter values, which are displayed in this list box.

SNo.	Local Domain	=>	SMTP Server IP Address	Port	Authenticat	User Name	P
1	mwti	=>	203.124.136.19	25	0		

Meanings of fields are given below:

Local Domain Name of local domain is displayed.

=> Symbol shows that the local domain maps to the SMTP Server IP address, shown in the next field.


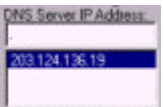
SMTP Server IP Address Displays Remote SMTP Server IP. Mails to the local domain are sent to this IP address of SMTP server.

Port Displays port number

Authentication Displays flag for authentication to gain access. Number 1 means that authentication is enabled and Number 0 means that authentication is not enabled.

User Name Name of user accessing SMTP server

Password Displays password to gain access.

Field Name	Description
	<p>Double click in the display box to view Edit Local Domain to IP Mapping.</p> <p>Enter values in the fields. Meanings of fields have been explained in the previous table.</p> 
Flush DNS	Select the button to flush dynamically resolved connections to the remote SMTP Servers. When a mail is sent to other domains, the SMTP server finds information like IP and Port numbers of the remote domains. These are stored in the registry before mails are sent.
Configuration for Outbound Mails:	
Reject unauthorized relaying	Select the check box to prevent SMTP server from relaying mails other than those listed in the relay list. This allows you to control Spammers.
DNS Server IP Address	When mails are sent to Internet, SMTP server needs to find IP of domain. It connects to a DNS server and finds information about the domains. Display box shows a list of all DNS server IPs, selected for query. Enter the DNS server IP in the field, to which the SMTP server directs queries. Select Add . The name is displayed in the display box.
	
Allow Relay from ONLY from User/IP	Field allows you to specify a names or IP of users and domains that are allowed to relay mails through your SMTP server. List box displays names. To add a name: Enter value in the field and select Add .

SMTP Spam – General Configuration

Your SMTP server will receive requests from multiple clients, a majority of which may be genuine users while some may be Spammers. The SMTP Spam Configuration allows you to configure your SMTP server for maximum Spam control. There are two main tabs: General Configuration and SMTP Configuration.

The General Configuration has tab pages that allow you to Substitute Domains, control mails sent and received by users, configure SMTP settings and Controls and set acknowledgement and routing by users.

- [SMTP Settings](#)
- [SMTP Controls](#)

- [Substitute Domains](#)
- [Mails From Users](#)
- [Mails to Users](#)
- [Acknowledgment & Routing](#)

The tab pages are explained in the next sections.

SMTP SETTINGS

The tab allows you to configure settings for SMTP incoming and outgoing emails. You assign the maximum number of incoming threads, set the retry levels for undelivered mails, etc.

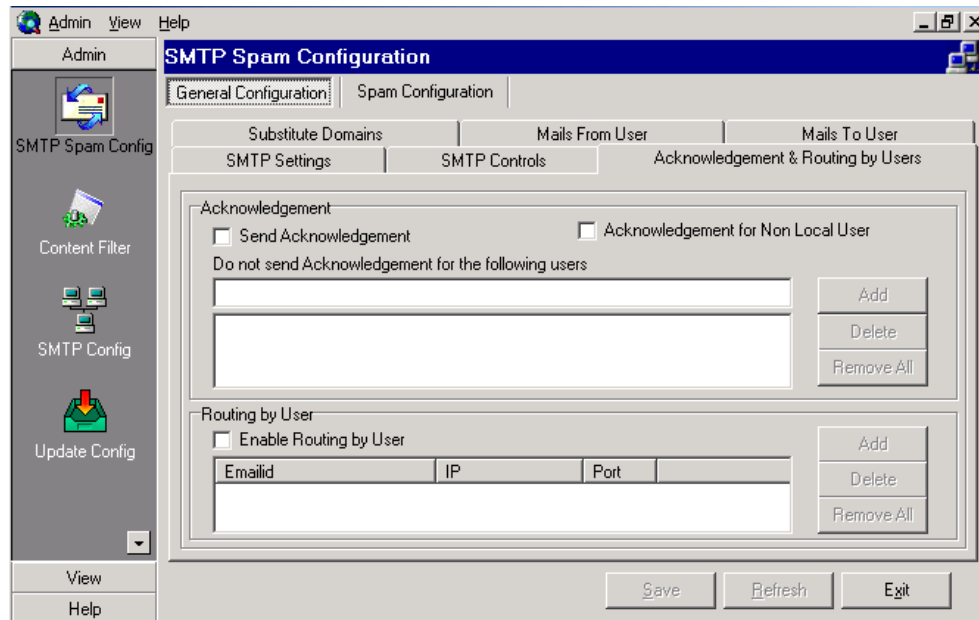


Figure 7.2 SMTP Settings

Field Name

Description

SMTP Incoming: Frame allows you to configure settings for SMTP incoming mails.

Maximum Incoming Threads Defines number of simultaneous incoming connections from remote SMTP Server. Default value is set at 32. Use the spin button to increase or decrease incoming connections. Number of connections allowed depends on machine configuration.

SMTP Server to Enter port number of SMTP through which all mails are received.

Field Name	Description
Listen on Port :	
Allow Connections coming in on any interface	A PC may have multiple IPs with a single network card or multiple IPs with multiple network cards. Select the radio button to allow any IP to interact with the remote SMTP Server.
Bind To IP	Select the radio button to bind an IP to the SMTP Server. Drop-down list box allows you to select an IP. Fields “Allow Connections coming in on any interface” and “Bind To IP” are mutually exclusive.
SMTP Outgoing:	Frame allows you to configure settings for SMTP outgoing mails.
Send EHLO	EHLO in Simple Authentication Security Layer (SASL) responds with a list of SMTP extensions that it supports. This allows SMTP server to authenticate a client.
Retry Delays In Minutes	While sending mails, if the connection is not successful, the SMTP Server retries to send mail as per the time interval in minutes, displayed in the display box. Display box displays the retry levels.
Warning When Entering Level	When SMTP Server shifts to the next retry level to send queued mails, a warning is sent informing system administrators.

SMTP CONTROLS

The SMTP Controls tab page allows you to set the RCPT limit. Other features available in the screen include: setting size restriction for e-mails, mail parking - where you set the mail parking time and size for e-mails that need to be parked and mail delay - where you set the delay time after which e-mails are forwarded.

Mails with large attachments consume valuable bandwidth. During peak time, such large mails hit the normal business work. Such mails can be ‘parked’ for a while in the server and sent at a scheduled time during off-peak hours. This is called **mail parking**.

Sometimes, after you send a mail, you may need to stop it, before it is forwarded to the recipient. **Mail Delay** allows you to specify the delay time, before a mail is actually sent from the server.

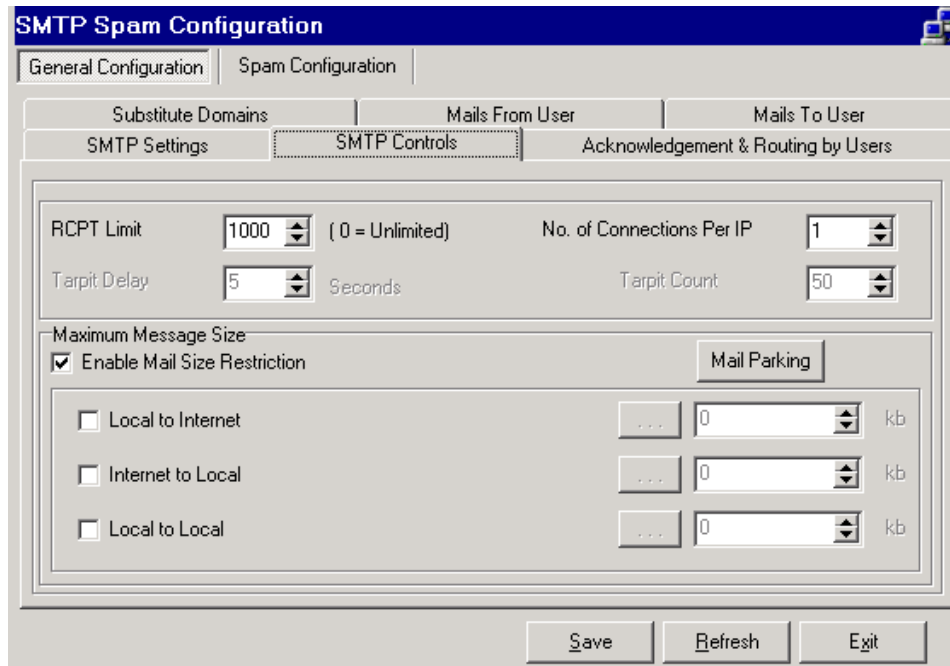


Figure 7.3 SMTP Controls

Field Name	Description
RCPT Limit	RCPT (Recipient Address) Limit defines the number of recipient addresses that can be added to an envelope. When mails are received, the SMTP Server keeps track of an envelope for a recipient. The envelope has a number of recipient addresses and a return path. Set the RCPT Limit using the spin button. Zero value means that there is no limit.
No. of Connections Per IP	Select the number of connections allowed for an IP, using the spin button. One connection is set by default.
Tarpit Count	Tarpit takes over unused IP addresses on a network and creates "virtual machines" that answer to connection attempts by Spammers and hackers. Tarpit answers those connection attempts in a way that causes the machine at the other end to get "stuck", sometimes for a very long time. SMTP Tarpit slows down the SMTP server as the number of recipient's increases. Also once the number hits a fixed amount (e.g. 100) it refuses to send the email. This prevents local users, using your mail server as an exploder for SPAM. While you can cut them off once you find out, the damage is usually done. Tarpit slows them down to the point of being unusable, making them change to delivering 1 message per connection. If you then transparently route all SMTP through your mail server, your users can never use your service to Spam
Tarpit Delay	Defines delay in seconds the SMTP servers does before relaying a mail.
Mail Parking	Select the button to view Mail Parking & Delay for Outbound Mails

Field Name	Description
	dialog box. The box allows you to select the size of e-mails that should be parked or delayed and set the time duration for this action.

There are two frames: Mail Parking and Mail Delay.



Mail Parking

Enable Mail Parking: Select the check box to allow mail parking in your mail server. Other fields in this frame are enabled only if the check box is selected.

Mails above size: Set the size of e-mails that should be parked. Select the size in Kb from the spin box. All e-mails, greater than the selected size will be parked.

Send after time: Spin box allows you to set the time in hours and minutes for mail parking.


Mail Delay

Enable Mail Delay: Select the check box to allow mail to be delayed before they are forwarded. Other fields in this frame are enabled only if the check box is selected.

Send outgoing mails after delay: Spin box allows you to set the mail delay time in minutes.

Above options applicable for High-Priority emails: Select the check box to apply above settings for e-mails classified as high priority.

Enable Mail Size Restriction	Select the checkbox to allow size restriction for e-mails sent or received in your network. Other fields in the frame are enabled only if the check box is selected.
-------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Local to Internet	Select the check box to restrict size of e-mails sent from your local domain to the Internet. Click  to open the Individual Size Restriction box. This box allows you to restrict mail size of specific users. To add email IDs, click Add and enter email ID of the user in the Addition / Modification box. Set the max mail size that the user can send and select OK .
--------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

In the adjacent spin box set the maximum size in Kb of the e-mail that can be allowed. Default value Zero, signifies that there is no restriction for e-mail size.

Internet to Local	Select the check box to restrict size of e-mails sent from the Internet to
--------------------------	----------------------------------------------------------------------------

Field Name	Description
	<p>your local domain. Click <input type="button" value="..."/> to open the Individual Size Restriction box. This box allows you to restrict mail size of specific users. To add email IDs, click Add and enter email ID of the user in the Addition / Modification box. Set the max mail size that the user can send and select OK.</p> <p>In the Internet tab, in the adjacent spin box set the maximum size in Kb of the e-mail that can be allowed. Default value Zero, signifies that there is no restriction for e-mail size.</p>
Local to Local	<p>Select the check box to restrict size of e-mails sent from Local to Local domain. Click <input type="button" value="..."/> to open the Individual Size Restriction box. This box allows you to restrict mail size of specific users. To add email IDs, click Add and enter email ID of the user in the Addition / Modification box. Set the max mail size that the user can send and select OK.</p> <p>In the Internet tab, in the adjacent spin box set the maximum size in Kb of the e-mail that can be allowed. Default value Zero, signifies that there is no restriction for e-mail size.</p>

SUBSTITUTE DOMAINS

The Substitute Domains tab allows you to substitute a domain with another domain. This is used when you wish to redirect mails from domain to another domain. This feature is useful when an existing domain does not exist or needs to be replaced.

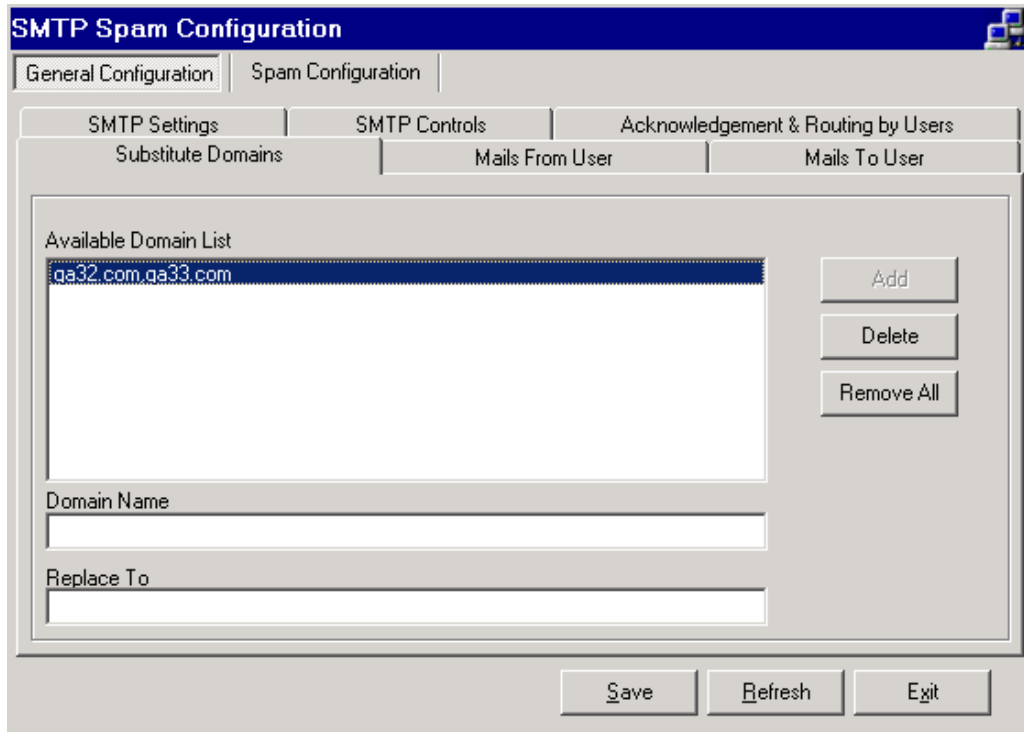


Figure 7.4 Substitute Domains

Field Name	Description
Available Domain List	<p>Display box shows a list of source and replaced domain names. For e.g. spaminfo.com, latestupdate.com means that you have replaced spaminfo.com with latestupdate.com</p> <p>To substitute a domain name:</p> <p>Enter domain name to be replaced in the Domain Name field. Next, enter the replacement name in the Replace To field. Select Add. The names appear in the display box.</p>
Domain Name	Enter domain name you wish to replace. The name entered here will be replaced with the name specified in 'Replace To' field.
Replace To	Enter domain name you wish to replace with. The name entered here will replace the name specified in 'Domain Name' field.

MAILS FROM USERS

The Mails From Users tab page allows you to send a copy of mails received from a user or domain to an e-mail ID or domain. You can also specify the route or IP address used to send the copy.

Figure 7.5 Mails From User

Field Name	Description
Mails from Users/Domain	Field allows you to enter user ID or domain, copy of mails received from them should be sent to another user or domain.
Send Copy To	Enter e-mail ID or domain IP to which copy of e-mails are sent.
Mails from Users/Domain	Field allows you to enter user ID or domain, mails received from them are routed through the domain.
Route To	Enter domain IP through which e-mails are routed.

MAILS TO USERS

The Mails To Users tab page allows you to send a copy of mails sent to a user or domain to an e-mail ID or domain. You can also specify the route or IP address used to send the copy.

Figure 7.6 Mails To Users

Field Name	Description
Mails To Users/Domain	Field allows you to enter user ID or domain, copy of mails received by them, should be sent to another user or domain.
Send Copy To	Enter e-mail ID or domain IP to which copy of e-mails are sent.
Mails To Users/Domain	Field allows you to enter user ID or domain, mails received by them are routed through the domain.
Route To	Enter domain IP through which e-mails are routed.

ACKNOWLEDGEMENT & ROUTING BY USERS

This tab allows you to configure settings that send an acknowledgment to users when mails are delivered or the SMTP Server fails to deliver the message.

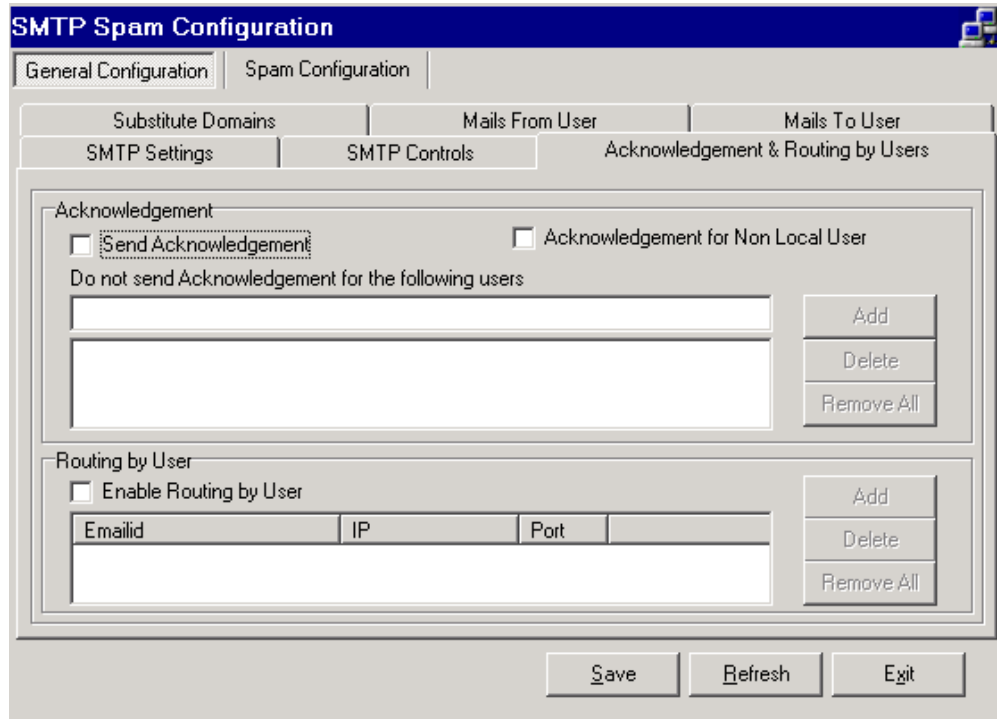
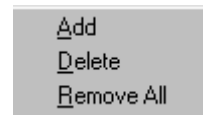


Figure 7.7 Acknowledgment & Routing by Users

Field Name	Description
Send Acknowledgment	Select the check box, to send acknowledgment to users. The acknowledgment is sent when messages are delivered.
Acknowledgment for Non Local User	Select the check box, to send acknowledgment to non-local users who request access from another domain. The acknowledgment is sent when messages are delivered.
Enable Routing by User	Select the check box to enable routing of mail by users. Display box lists all e-mails IDs, their IP and port number of users that are allowed to use the routing feature. Right click in the display box to view a pop up.



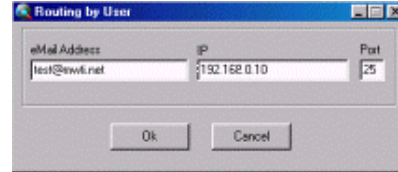
Select **Add** to view **Routing by User** dialog box.

Field Name	Description
------------	-------------

eMail Address: Enter e-mail ID of user who is allowed to route mails.	
------------------------------------------------------------------------------	--

IP: Enter IP address used for routing.	
-----------------------------------------------	--

Port: Enter port number used for routing.	
--------------------------------------------------	--



SMTP Spam – Spam Configuration

Your SMTP server will receive requests from multiple clients, a majority of which may be genuine users while some may be Spammers. The SMTP Spam Configuration allows you to configure your SMTP server for maximum Spam controls. There are two main tabs: General Configuration and SMTP Configuration.

The SMTP Configuration tab has different tabs that allow you to specify which users are allowed or barred from sending and receiving mails: configure the real-time black hole lists; set the Spam SMTP controls and set authentication for users.

- [Authentication](#)
- [Internet](#)
- [Restriction From Users](#)
- [Restriction To Users](#)
- [RBL / DUL Settings](#)

Details are explained in the next sections.

AUTHENTICATION

SMTP Servers are used by millions of hosts around the globe. For quite sometime, it functioned on the inherent levels of trust among members of the net community and lacked robust authentication procedures. This flaw, coupled with both the default policies of many SMTP implementations and the ease of spoofing the IP protocols, resulted in widespread abuses of the SMTP infrastructure.

This lack of authentication capability is a two-way problem: the SMTP server is unable to verify that the client is genuine; the SMTP client is unable to trust that the SMTP server is genuine.

The Postfix mail system's wide variety of configuration options help administrators combat abuse by allowing precise restriction of the server's resources and how they are made available for the use of others. These mechanisms rely upon one of two authentication methods: IP address and DNS information.

The Authentication tab page allows you to set up authentication options for X-Spam. These allow the server to authenticate a client and also permit the client to confirm if the SMTP server is genuine. Authentication allows system administrators to fight mail abuse, identify and block Spammers.

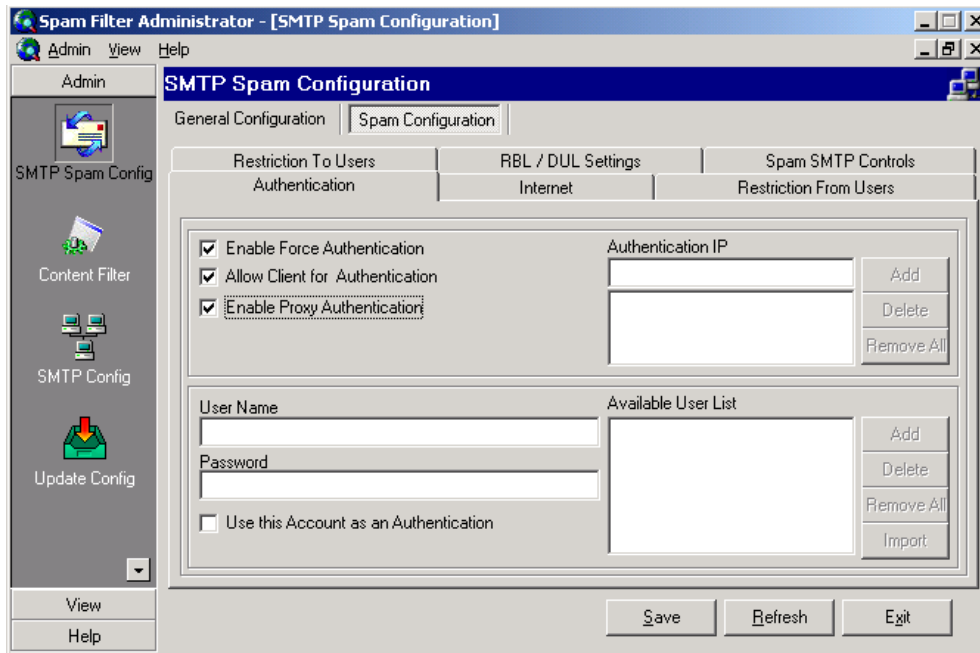


Figure 7.8 Authentication

Field Name	Description
Allow Client for Authentication	Select the check box to allow clients authentication.
Enable Proxy Authentication	Select the check box to authenticate the proxy used by clients.
Enable Force Authentication	Allows you to force an authentication process on clients. If authentication fails, access is refused.
Authentication IP	Enter client IP that needs to be authenticated.
Available User List	Display box lists all authenticated users, allowed access to the SMTP Server. User name and password are displayed. Process of adding users is explained in the next two fields.
User Name	Enter user name in this field. The name is displayed in the “Available User List”.
Password	Enter password for user name, in this field. The password is displayed in the “Available User List”. This feature is useful when you add new users. Individual users first time login using the password you have assigned which can be changed later.

Field Name	Description
Import	Allows you to import a list of domains and users. Names are displayed in the list box. The first set of values have a suffix "1".
Use this Account as an Authentication	In the display box, click the account to be used for authentication and select the check box.

INTERNET

The Internet tab page allows you to specify users that should be stopped from receiving or sending e-mails through the Internet. This feature is useful to block known Spammers from using your mail server to launch Spam.

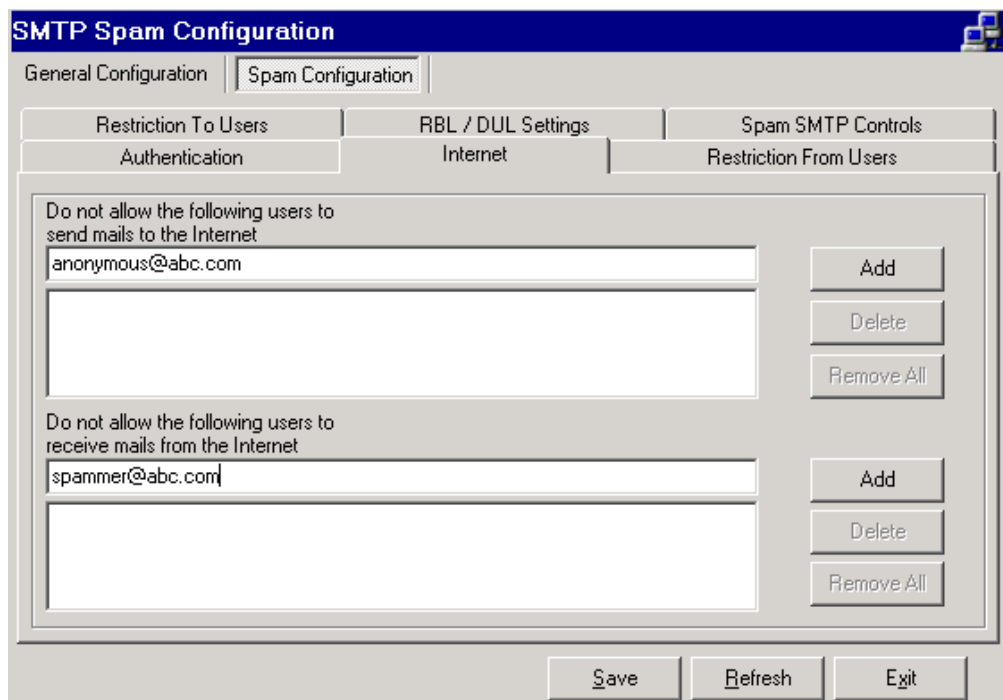


Figure 7.9 Internet

Field Name	Description
Do not allow the following users to send mails to the Internet	Frame allows you to stop a user from <i>sending</i> e-mails through Internet. Enter e-mails IDs of users who should not be allowed to send e-mails to the Internet, in the top field and select Add . The ID is displayed in the display box. To remove the name from the list, click on the name and select Delete .

Field Name	Description
Do not allow the following users to receive mails from the Internet	Frame allows you to stop a user from <i>receiving</i> e-mails through Internet. Enter e-mails Ids of users who should not be allowed to send e-mails to the Internet, in the top field and select Add . The ID is displayed in the display box. To remove the name from the list, click on the name and select Delete .

RESTRICTION FROM USERS

The tab allows you to specify users or Hosts IP of users whose mails can be allowed or blocked in your SMTP Server. You can apply restrictions to mails from users.

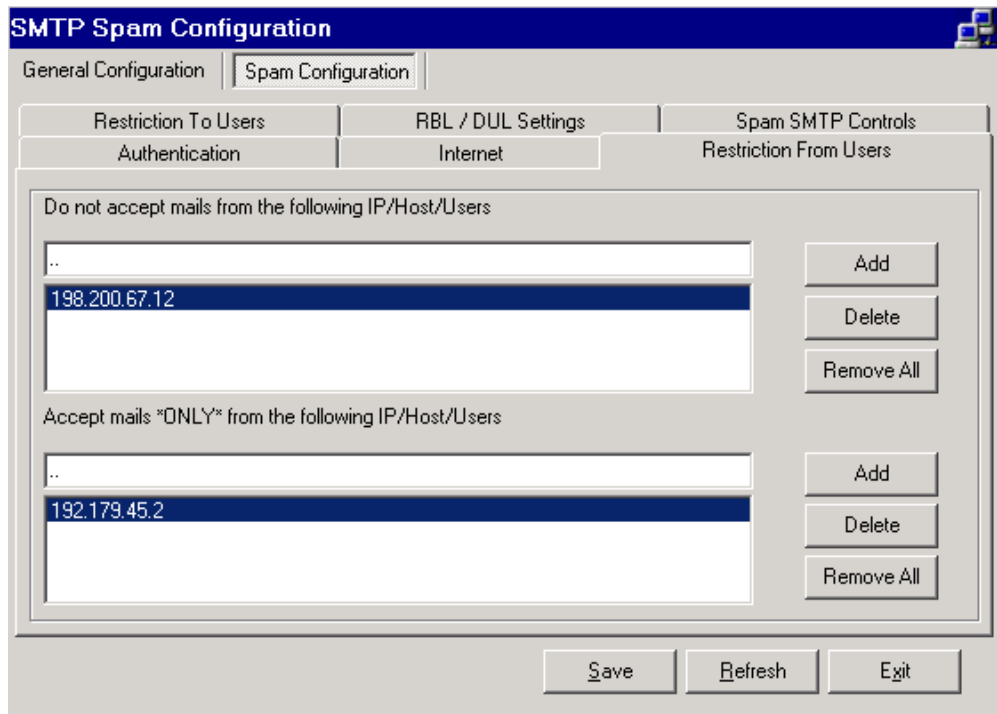


Figure 7.10 Restriction From Users

Field Name	Description
Do not accept mails for following Host/Users	Frame allows you to specify IP/Host or user e-mails IDs whose e-mails need to be <i>blocked</i> . Enter IP or e-mails Ids of users in the top field and select Add . The IP/ID is displayed in the display box. To remove the name from the list, click on the name and select Delete .
Accept mails 'ONLY' for following	Frame allows you to specify IP/Host or user e-mails IDs whose e-mails are <i>allowed</i> . Enter IP or e-mails Ids of users in the top field and select Add . The IP/ID is displayed in the display box. To remove the name from the

Field Name	Description
IP/Host/Users	list, click on the name and select Delete .

RESTRICTION TO USERS

This tab allows you to specify e-mails IDs or Hosts IP of users whose mails can be allowed or blocked. You can apply restrictions to users mails.

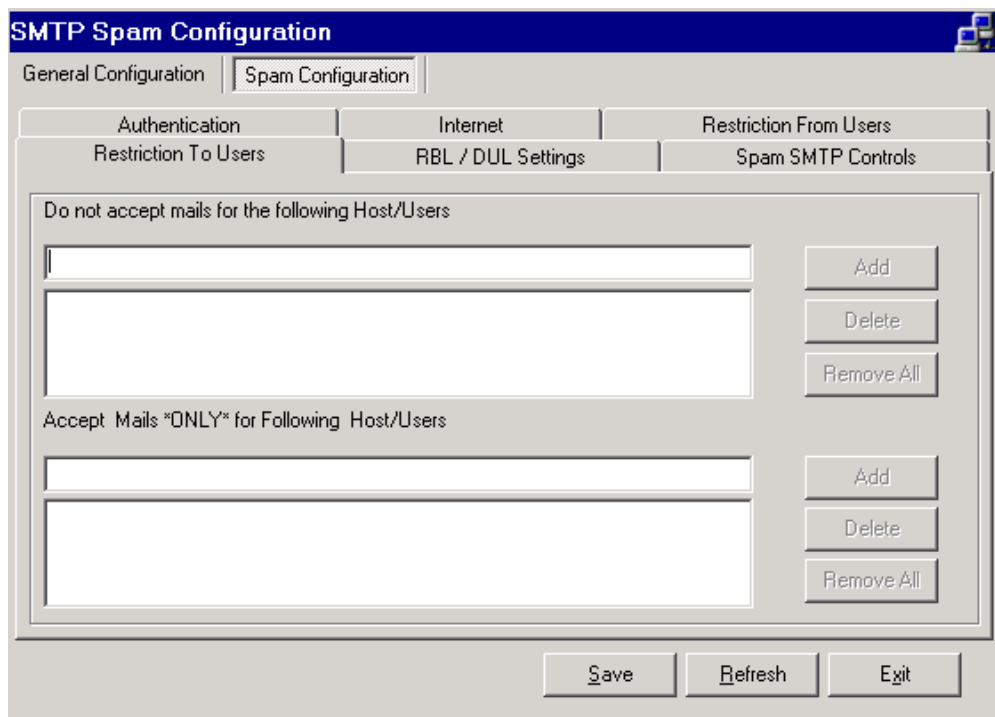


Figure 7.11 Restriction To Users

Field Name	Description
Do not accept mails for following Host/Users	Frame allows you to specify IP/Host or user e-mails IDs whose e-mails need to be blocked . Enter IP or e-mails Ids of users in the top field and select Add . The IP/ID is displayed in the display box. To remove the name from the list, click on the name and select Delete .
Accept mails 'ONLY' for following Host/Users	Frame allows you to specify IP/Host or user e-mails IDs whose e-mails are allowed . Enter IP or e-mails Ids of users in the top field and select Add . The IP/ID is displayed in the display box. To remove the name from the list, click on the name and select Delete .

RBL / DUL SETTINGS

This tab page allows you to configure settings that provide protection against Spam. Spammers can use your SMTP Server to launch Spam attacks. Checks can be run to verify if the user who requests access is listed in the Realtime Blackhole List and the Dial Up User list.

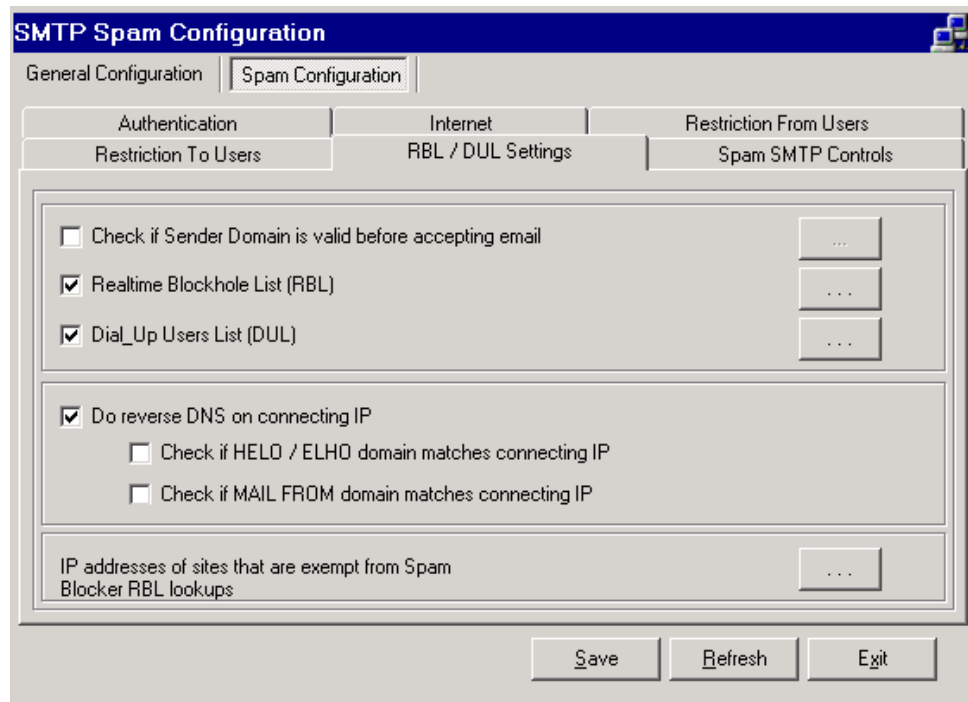




Figure 7.12 RBL / DUL Settings

Field Name	Description
Check if Sender Domain is valid before accepting email	Select the check box to verify if the sender domain is valid, before accepting e-mail. Click <input type="button" value="..."/> to open the Select dialog box. You can ensure that the following items are checked. Check A-Record: Checks all A type of records. Check MX-Record: Checks MX type of records. Check both A and MX-Records: Checks both types.
Realtme Blackhole List (RBL)	Organizations like MAPS (Mail Abuse Prevention System) provide a list of IP addresses that are known Spammers. This list is called Realtme Blackhole list. When a suspicious client requests access to the SMTP server, you can send the IP address to the MAPS list, which returns the request after verifying the authenticity. Select the check box to check with the RBL and verify if the sender domain is valid, before accepting e-mail. Click <input type="button" value="..."/> to open the Realtme Blackhole List (RBL) dialog box. A list of addresses that carry details of known Spammers is displayed. Enter the suffix to add to

Field Name	Description
	the IP address for queries and click Add .
Dial_Up Users List (DUL)	Spammers sometimes use stealth mail tactics when their initial Spam attempts are blocked. They use a dial-up-service (DUL) provider to connect their Spam mail service, to the SMTP Server. This is trespassing on your MailServer and the MAPS DUL project helps in identifying and stopping Spam. The project has a list of DUL users who are known Spammers. To verify if the request for connection to your SMTP Server is genuine, you can send a query to dialups.mail-abuse.org . The request is verified and returned.
	Spammers use a dial up service to send Spam. Organizations maintain a list of known Spammers. Click  to open the Dial_Up Users List (DUL) dialog box. A list of addresses that carry details of known Spammers is displayed. Enter the suffix to add to the IP address for queries and click Add .
Do reverse DNS on connecting IP	When other users try to connect to your server, you can run a reverse DNS to verify their IP.
Check if HELO/EHLO domain matches connecting IP	This is a request made to the SMTP server by a client. This allows SMTP Server and its client to verify each other's authenticity. The request from the client is in the form of a parameter with the clients name or IP address.
	SMTP Server responds with a text message and its name or IP and its abilities. Some servers reject messages from clients whose HELO parameters do not match the results of PTR lookups on their IP addresses
Check if MAIL FROM domain matches connecting IP	Spammers send mails through another IP. This check verifies if the IP in the From field is the same as the connecting IP.
IP Addresses of the sites that are exempt from Spam RBL lookups	Certain well-known sites like www.mwti.net are authentic and you can exempt them from RBL look ups. Click  to open the Exception IP List dialog box. You can enter IP of sites that are exempt from RBL lookups.

SPAM SMTP CONTROLS

This page allows you to set Spam controls for the SMTP server. You can choose to send emails, line by line and also specify extra characters in email IDs that Spammers sometime use to send Spam.

Field Name	Description
Send Mail Line By Line	Select the check box to send e-mails line-by-line. This ensures that the highest clarity is retained in the forwarded e-mails but time taken is more. If the check box is not selected, then data is sent in packets.
Show Progress After Bytes	Spin button allows you to select size in Kb after which the progress bar for outgoing or incoming mails is refreshed.
Extra Char in email ID	Field allows you to specify extra characters used in the e-mail ID. Mails that have any of these characters in the "To" address are not downloaded by the Server, but rejected outright. This feature helps to fight Spam.

Content Filter

The Content Filter menu is the main X-Spam engine. It allows you to define rules for mails to be considered as Spam. Each rule is assigned a score and you can set the total threshold positive and negative score. Test can then be run for the defined rules. If the total score touches the threshold, then the mail is regarded as Spam.

Regular Expressions are used to test for Spam. MicroWorld provides a set of standard regular expressions. The rules or regular expressions can be automatically downloaded as per a schedule. This ensures that your X-Spam is stocked with the latest rules to identify Spam and block Spam. You can even set customized regular expressions to define new rules and assign them a score.

There are different tabs that allow you to refine your rules and tests.

- [Action](#)
- [Heuristic Options](#)
- [Regular Expression Tests](#)
- [Meta Tests](#)
- [White / Black List](#)

The next sections provide detailed information.

ACTION

The Action screen allows you to identify and segregate Spam. You can choose to add a Flag in header and subject of mails identified as Spam. Such mails can then be auto deleted or forwarded to a specific folder in your mailbox.

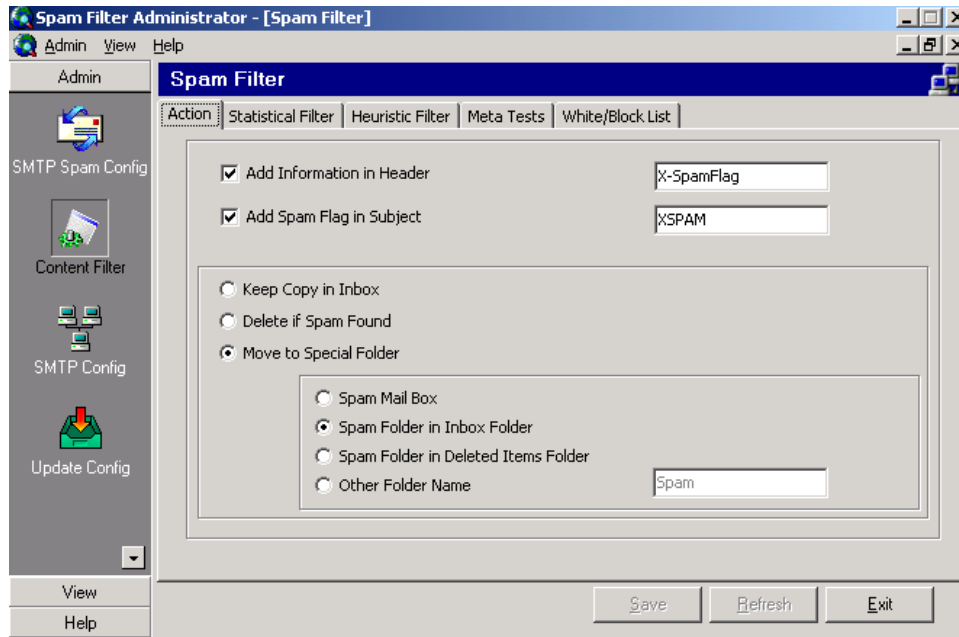


Figure 7.13 Action for Spam

Field meanings are described in the following table. Select the check boxes or radio buttons to enable the fields.

Field Name	Description
Add Information in header	An X-Spam Flag can be added to the Spam header. Your mail service reads this flag and either deletes it or stores it in a safe folder. Select the checkbox to enable the adjacent data entry field and enter the flag name. The name can be alphanumeric and of 25 characters. Use only underscores or hyphens to separate words.
Add Spam Flag in subject	An X-Spam Flag can be added to the Spam subject. Your mail service reads this flag and either deletes it or stores it in a safe folder. Select the checkbox to enable the adjacent data entry field and enter the flag name. The name can be alphanumeric and of 25 characters. Use only underscores or hyphens to separate words.
Keep Copy to inbox	When Spam is detected it can be kept in your inbox. You can later delete or use it.
Delete If Spam found	When a mail is identified as Spam, you can choose to automatically

Field Name	Description
	delete it.
Move to special folder	Spam is moved to a special folder in your mailbox. The bottom frame is enabled only if this radio is selected. You can choose the following options: <p>Spam mailbox: Spam is copied in the Spam folder of your mailbox.</p> <p>Spam folder in inbox folder: A special folder called Spam is created in your inbox. Spam mails are copied into this folder.</p> <p>Spam folder in deleted items folder: A special folder called Spam is created in your deleted items folder. Spam mails are copied into this folder.</p> <p>Other folder name: You can create a special folder and assign it a name. The adjacent field is enabled only if this option is selected. Enter the new name in this field.</p>

STATISTICAL FILTER

Statistical Filter allows you to select the type of regular expressions tests to be run. There are hundreds of different types of tests. When a mail tests positive for a rule then its score is added. You can choose to designate the mail at the first instance of a positive result or run tests for all regular expressions. You can also designate a mail as Spam once the threshold score limit is reached.

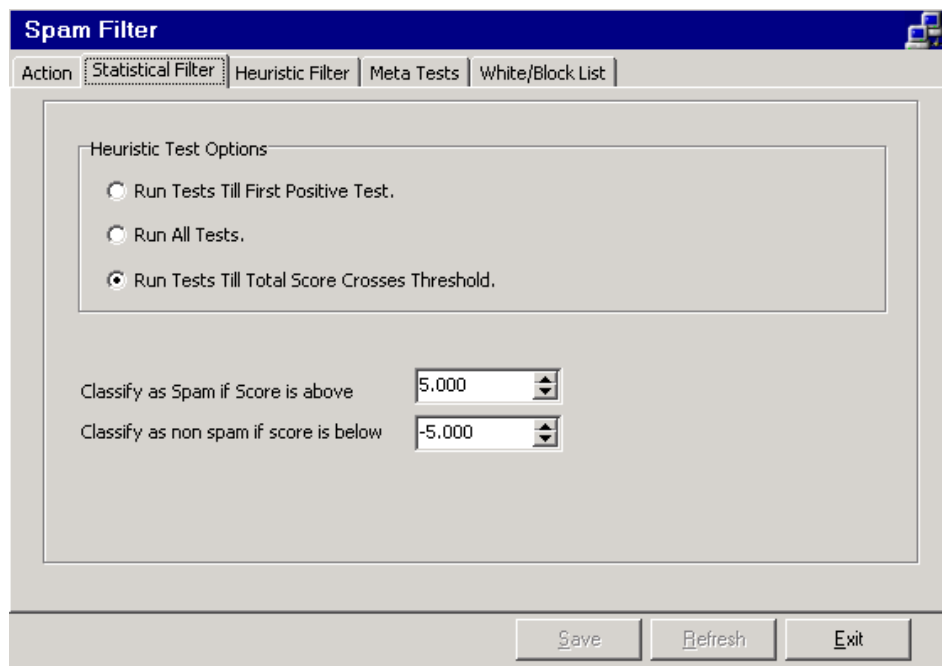


Figure 7.14 Heuristic Options

Field meanings are described in the following table. Select the check boxes or radio buttons to enable the fields.

Field Name	Description
Run Tests Till First Positive Test	This tests runs the regular expression tests and at the first instance of a positive result, the mail is designated as Spam.
Run All Tests	This test runs all the regular expressions tests and a total of all results is calculated. You can then designate the mail as Spam.
Run Tests Till Total Score Crosses Threshold	Tests are run with all the regular expressions and the results are added. When the results reach a threshold limit, the mail is designated as Spam.
Classify as Spam if score is above	The combo box allows you to set the Positive Threshold. If the positive score reaches this threshold then the mail is classified as Spam.
Classify as non Spam if score is below	The combo box allows you to set the Negative Threshold. If the negative score reaches the negative threshold then the mail is classified as Non Spam.

HEURISTIC FILTER

A huge list of predefined regular expressions is provided with X-Spam. These are displayed in the predefined list box. Each expression has a check box with a description. You can select the regular expression to be used for testing. Updates for the regular expressions are automatically downloaded as per the schedule you have assigned. This ensures that your X-Spam has the latest ones in place to help you combat Spam.

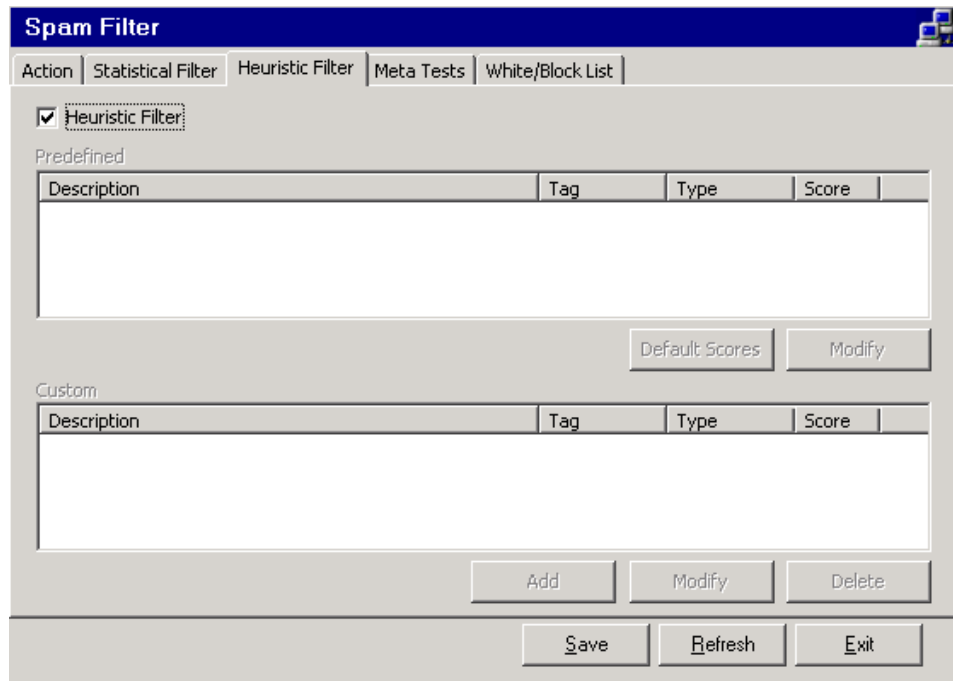


Figure 7.15 Regular Expression Tests

Field Name	Description
Heuristic Filter	Select the check box to run Heuristic Filter tests.
Predefined	<p>A huge list of predefined regular expressions is provided with X-Spam. These are displayed in the Predefined list box. Each expression has a check box with a description. You can select the regular expression to be used for testing.</p> <p>Description: Gives a brief description of the regular expression.</p> <p>Tag: Each test has a unique identifier tag that identifies the test..</p> <p>Type: Specifies the part of a mail where the regular expression is tested (body , header etc)</p> <p>Score: Depending on the severity, a score is given for a regular expression. When the test turns positive, the score is added to the total.</p>
Modify	<p>Select the button to view the Heuristic File Modification dialog box. The non-editable fields display the description, type and the regular expression.</p> <p>You can modify the score. To run the rule, select the Enable this rule check box.</p> <p>Click OK for the modifications to be applied.</p>
Default Scores	Pre-defined default scores are restored.
Custom	You can create and assign your own regular expressions. To add a custom regular expression, click Add. The Heuristic File Addition dialog box is displayed. The fields are described as below:

Field Name	Description
	<p>Description: Gives a brief description of the regular expression.</p> <p>Tag: Each test has a unique identifier tag that identifies the test.</p> <p>Type: Specifies the part of a mail where the regular expression is tested (body, header etc).</p> <p>Score: Depending on the severity, a score is given for a regular expression. When the test turns positive, the score is added to the total.</p> <p>To run the rule, select the Enable this rule check box. Click OK for the modifications to be applied.</p> <p>The regular expression is displayed in the custom display box</p>
Modify	<p>To modify a listed custom regular expression, select it and click on the button to view the Heuristic File Modification dialog box with the assigned values. The description field is non-editable. You can modify values in other fields.</p>
Delete	<p>To delete a custom regular expression, select it and click on the delete button.</p>

META TEST

Meta Tests allow you to run further tests to identify Spam. MicroWorld provides a list of predefined regular expressions. You can use a combination of multiple expressions with qualifiers like and, or, =, >, <, ! and so on. This feature provides an edge to your tests and ensures that even skillfully made Spam is detected. Meta test expressions are not regular expressions, but expressions comprised of other regular expression test tags and qualifiers. Their results depend on the all the regular expression tests that they contain.

The screen is only enabled if the Heuristic Filter check box in the Heuristic Filter tab is not selected.

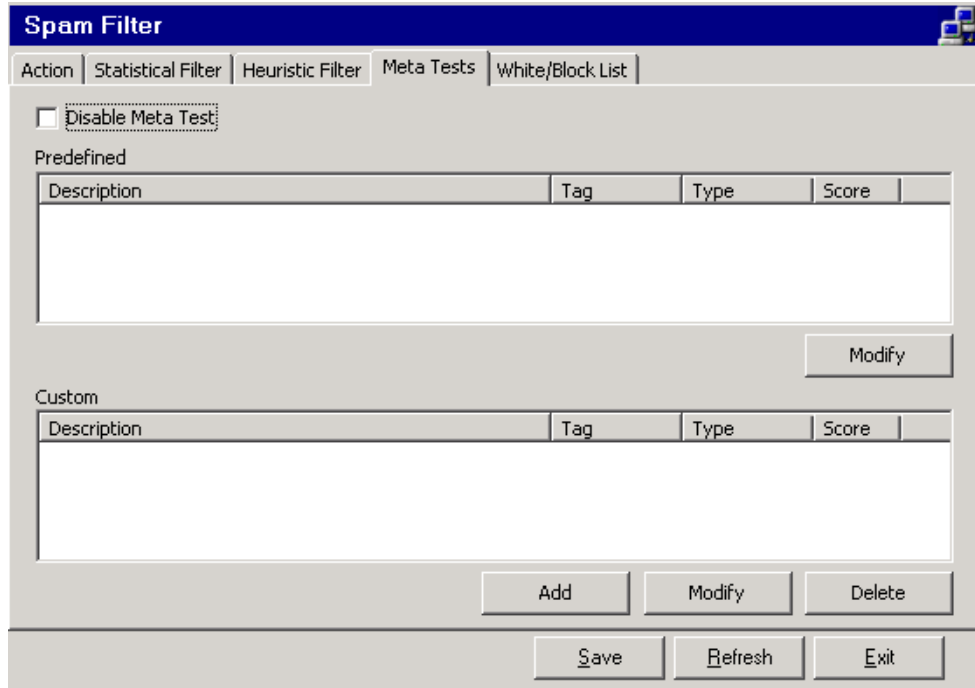



Figure 7.16 Meta Test

Field Name	Description
Disable Meta Test	If the check box is selected then the tab is disabled and you cannot validate any field in the tab.
Predefined	A huge list of predefined meta Tests is provided with X-Spam. These are displayed in the predefined list box. Each test has a check box with a description. You can select the meta tests to be used for testing. Description: Gives a brief description of the meta test. Tag: Each test has a unique identifier tag that identifies the test. Type: Specifies that it is a meta test. Score: Depending on the severity, a score is given for a meta test expression. When the test turns positive, the score is added to the total
Add	To add a combination of regular expression tests, click Add. The FrmMeta dialog box is displayed. Enter suitable values for Score and Description fields. Available Regular Expression tests are listed in the lower list box. To use the test in the meta test expression, double click it. It is now displayed in the Meta Test box. You can add multiple regular expression tests in the Meta Test box. To use them as a combination, select the test and click  . A small popup with commonly used qualifiers is displayed. Assign them as required.
Modify	To modify a combination of regular expressions, select it and click Modify. The MsgArray dialog box with previously assigned values is

Field Name	Description
	displayed. You cannot change the description. All other fields are editable.
Custom	You can create and assign your own combination of regular expressions. To add a custom regular expression, click Add . The FrmMeta dialog box is displayed. The fields are described in Predefined and Add .

WHITE / BLACK LIST

The menu allows you to create a white list of approved domains and users whose mails are allowed to enter or leave your server. At the same time, you can also create a black list of known Spammer domains and users whose mails are not allowed to enter or leave your server.

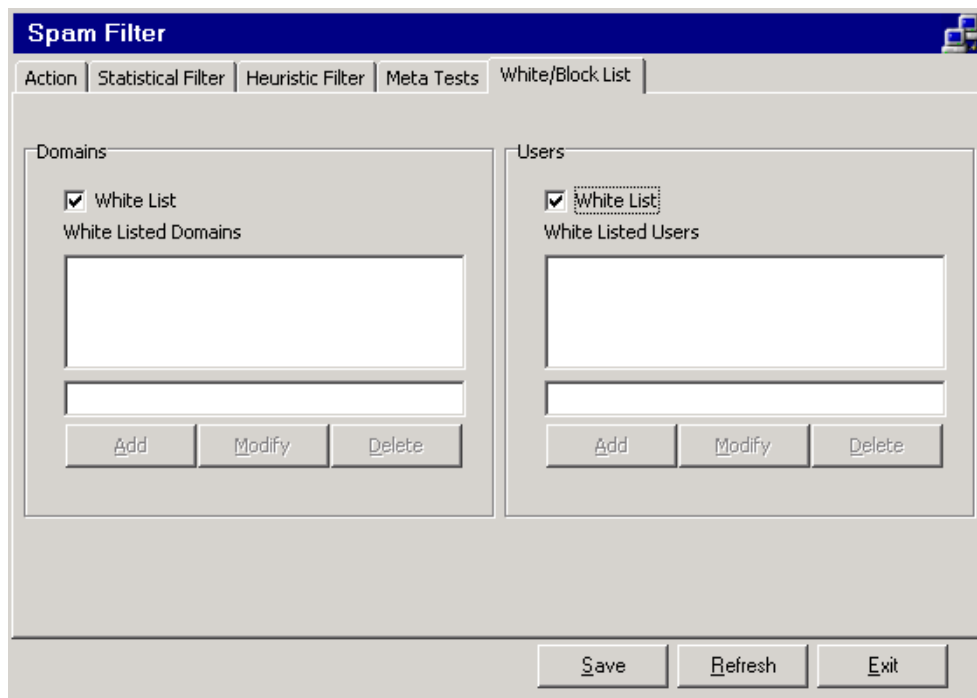


Figure 7.17 White / Black List

There are four frames in the screen that allow you to create white and black list for domains and users. To add domain names, IPs, URLs, email IDs to the list:

- Select the check box at the top of each frame
- Each frame has two parts. Click in the lower frame and type the domain name, IP, URL or email ID
- Click **Add**. The values you have entered are listed in the top part.

- To remove or modify a domain or user from the box, select the name and click on **Modify** or **Delete**
- Select **Save** and **Exit**.

Update Config

Update Config provides automatic downloads of updates. Updates are rules and tests created by MicroWorld to detect new spam. Updates are stored in our dedicated download mirror sites. When you install X-Spam, it checks your system and refreshes some of the fields in the eScan Updater user interface. MicroWorld has assigned the most optimum default values for download sites, mode of connecting to these sites, time interval for download of updates, etc. Change the values only if required.

This section provides details on setting up and configuring the settings for Updater. You assign the access mode your system uses to connect to the Internet, proxy IP addresses, time interval at which the system should download updates, etc. Typically the updates are up to 10 KB in size, so downloads are fast.

- [Set General Config](#)
- [FTP Config](#)
- [HTTP Config](#)
- [UNC Config](#)

SET GENERAL CONFIG

The **General Updater Configuration** screen allows you to select access mode, enable or disable download notification and auto downloads; download through proxy and assign the IP address of server from which downloads are done. You set the time interval for automatic downloads of updates from the Internet

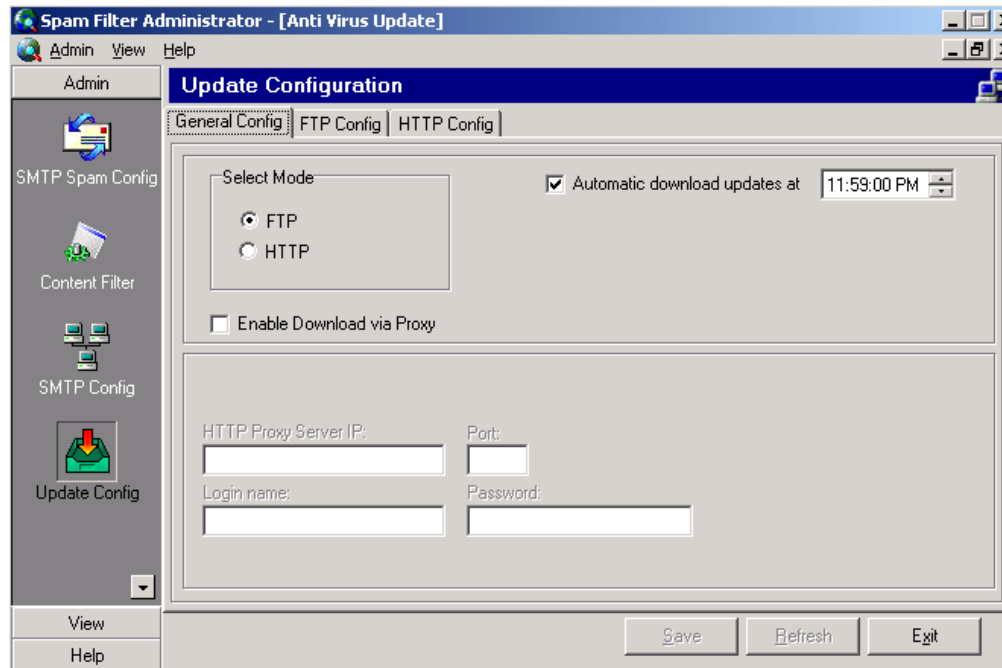


Figure 7.18 General Configuration

Field Name	Description
------------	-------------

Select Mode Updates are available on our designated mirror web sites. You connect to the mirror website and download updates using one of the connectivity modes. The three modes are: HTTP, FTP and UNC.

Set update download mode:

FTP (File Transfer Protocol) FTP offers the most stable means to transfer data. Use this mode when you have problems connecting using HTTP. Advantage with FTP protocol is that if connection breaks during download, it commences from the point where it broke in the previous attempt. Configuring FTP for a proxy server is more complicated when compared to configuring HTTP with the proxy-server. These are reputed to be slower than HTTP.

Select the radio button to download using FTP protocol. Tab page "FTP Config" is enabled only if this radio button is selected.

HTTP (Hyper Text Transfer Protocol): HTTP is the most commonly used access mechanism. The software selects it as the default mode. If connection is broken during download, you have to start from the beginning. HTTP downloads are faster than other types.

Select the radio button to download using HTTP mode. Tab page "HTTP Config" is enabled only if this radio button is selected.

Network (Universal Naming Convention) UNC is the standard for naming network drives. For example, UNC directory path has the following form: \\server\folder\subfolder\filename. In a network environment, when only one system has Internet connectivity and updates are to be transferred to many machines, choose this mode. If your machine does

Field Name	Description
	not have Internet access, you can choose any machine in the LAN and assign it to download updates. This ensures that updates are transferred to individual machines.
	Select the radio button to download using Network mode. Tab page "UNC Config" is enabled only if this radio button is selected.
Automatic download of Updates at	The spin button allows you to set the time when updates are downloaded automatically.
Enable Download Via Proxy	Select the check box if your mail server is behind a proxy server. The next four fields are enabled only if this check box is selected.
HTTP Proxy Server IP:	Enter the IP address of the HTTP Proxy server in this field. System downloads using this proxy. This field is enabled only if "Enable Download Via Proxy" check box is selected.
Port:	Enter the port number of the HTTP proxy server. This field is enabled only if "Enable Download Via Proxy" check box is selected.
Login name:	Specify the login name of the user. System allows access only for this login name.
Password:	Password ensures that only the above login name is allowed access. Enter a password in this field. It can be alphanumeric and must be of minimum six characters.

FTP CONFIG

File Transfer Protocol (FTP) offers the most stable means to transfer data. Use this mode when you have problems connecting using HTTP. Advantage with FTP protocol is that if connection breaks during download, it commences from the point where it broke in the previous attempt. Configuring FTP for a proxy server is more complicated when compared to configuring HTTP with the proxy-server. These are reputed to be slower than HTTP.

Fields in this tab are enabled only if FTP Config is selected as the download mode in General Configuration tab.

Figure 7.19 FTP Config

Field Name	Description
FTP Download Site:	<i>Select update download FTP site:</i> MicroWorld stores updates in dedicated FTP servers. The sites are predefined in the program and displayed in the drop-down list. Select the appropriate FTP site from the drop-down list. The application connects to this site to download updates. The default site is displayed in the field.
Download Directory	Updates are stored in the FTP sites in a specific directory. Based on the selection done in "FTP Download Site" the relevant directory name is displayed in the non-editable display field. Default directory name is displayed in the field. This is a non-editable display field.
Port	Enter the port number from which updates are downloaded.
FTP Proxy Server IP:	Enter the FTP proxy server IP address in this field. The application uses this proxy to download updates. The field is enabled only when "Enable Download via Proxy" check box is selected in "General Config" tab page.
Port	Enter the port number of FTP proxy server. The field is enabled only when "Enable Download via Proxy" check box is selected in "General Config" tab page.
Login Name:	Specify the login name for proxy authentication. System allows access only for this login name. If your proxy server does not require authentication, then retain the displayed default name "Anonymous". The field is enabled only when "Enable Download via Proxy" check box is selected in "General Config" tab page.

Field Name	Description
Password:	Password ensures that only the above login name is allowed to access the application. Enter a password in this field. It can be alphanumeric and must be of minimum 6 characters. The field is enabled only when "Enable Download via Proxy" check box is selected in "General Config" tab page.

Logon Type When a client connects to the Internet) via a proxy server, additional configuration is required to download the updates. The fields in this frame are enabled only when "Enable Download via Proxy" check box is selected in "General Config" tab page.

Select Logon type:

User@siteaddress	This is the format the proxy or the Firewall between the client and the Internet that expects the logon command. Select the radio button if proxy used is WinGate, Winproxy, etc.
OPEN siteaddress	This is the format the proxy or the Firewall between the client and the Internet that expects the logon command. Select the radio button if logon type is Cproxy, etc.
PASV Mode	When you attempt to connect to the server, if a Firewall is present, it filters unwanted data and connection may not be granted. By using the passive or PASV mode, the server opens a random port, unsecured by the Firewall and allows you to connect. Select the radio button if logon type is of Firewall type.
Socks	Select the radio button if Socks proxy is used as the logon type. The drop-down list box is enabled only if the radio button is selected. Version specification numbers for the Socks Server are displayed in the drop-down list. Select the appropriate value.

HTTP CONFIG

This tab allows you to change the default settings for HTTP mode of download. The fields are enabled only if HTTP is selected as the mode in “General Config” tab page

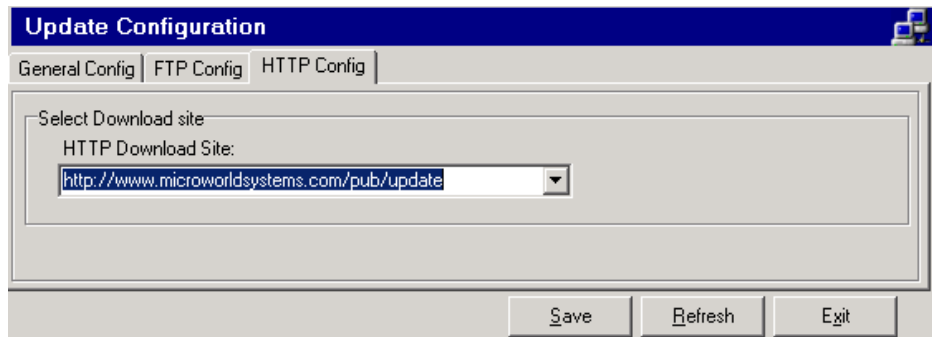


Figure 7.20 HTTP Config

Field Name	Description
HTTP Download Site:	A list of HTTP download sites for the application is displayed in the drop-down list. Select the appropriate site. The default HTTP site http://www.microworldsystems.com/pub/update is displayed in the field.

View

The view menu allows you to view log files of update log and also the download log. You can flush the Log, mail debug information and look at the reports of x-Spam activity.

- [View Log File](#)
- [Flush Log](#)
- [Mail Debug Information](#)
- [Report](#)

View Log File

The menu allows you to view the Download Log and the Auto Update Log.

VIEW DOWNLOAD LOG

Displays details of files downloaded as per the schedule

VIEW UPDATE LOG

Displays the update log. Details of when X-Spam was started and the version number of your X-Spam are listed.

Flush Log

Your log is flushed; old entries are refreshed with new values.

Mail Debug Information

You can report any bugs or problems, directly to support of MicroWorld. Select the link to view the “**Please type your problem**” entry box. Enter the details and click OK. The report is mailed to our support team who analyzes your problem and provides you with a solution.

Report

This feature provides a report of MailScan activity for a period. You can select the date range for which reports are generated. Click **Details** to view a popup with tabs that allow you to generate reports on different topics.

Mails Sent From Local Domains: Select date to view details of mails sent from the local domain. Details displayed include: domain name from which e-mails are sent, user or person sending e-mails, total number and size of all e-mails sent by the user.

Mails Received from Foreign Domains: Select date to view details of mails received from Foreign Domains. Details displayed include: Foreign domain name from which e-mails are received, total number and size of e-mails sent to the user and attachment infected.

Mail Details: Select date to view details of e-mails sent to a user in your system. Details displayed include: date message is sent, senders name, domain name from which e-mails is sent, message size in bytes, e-mail subject, recipient details, attachment name and size.

Alt. Detail: Select date to view other details of e-mails sent to a user in your system. Details displayed include: attachment file name, size and extension, total infections or virus in the file and if infected number of virus deleted or cleaned.

Mails Received by Local Users: Select date to view details of mails received by local users. Details displayed include: domain name from which e-mails are received, user or person sending e-mails, total number and size of all e-mails sent to the user and number of infections detected.

Daily Analysis: Select date range to view details of mails received and sent through your system. For a date, details displayed include: total mails sent and received, total mails sent and size in bytes, total mails received and size in bytes, total number of infections and how many mails were cleaned and deleted.

Common features of tab pages are described below. Fields and features may appear in only some of the tab pages.

Field Name	Description
From Date/To Date	You can select the range of dates to be covered in the report. Click on the drop-down list to open the calendar and select the dates. Report will display details for the period you select for the From and To fields. These two fields are available only for "Daily Analysis" report. Other tab pages have only a single date field and the report is generated for the selected date.
Filter	Filters the report for the selected date range.
S. No	Represents the serial number of the activity.
Msg Date	Date the message was sent.
Total Mails	Total number of mails sent and received during the period
Mails Sent	Total number of e-mails sent during the period.
Mail Sent in Bytes	Mails sent size in Bytes
Mails Received Bytes	Total e-mails received
Attachments Infected	Displays total number of infected attachments.
Spam	Displays number of Spam mails that were detected.

Help

The following menus are provided.

- [Test Spam](#)
- [Spam Help](#)
- [License Information](#)
- [Change Password](#)
- [About](#)

Test Spam

You can send a test Spam to find if X-Spam is installed properly. Select the link to view the **Send test Spam Mail** dialog box. Details of your SMTP Server IP, IDs of sender and receiver are displayed. Click **Send**.

If X-Spam is correctly installed, then as per the settings you have done in Heuristic Filter, the Spam is detected and the preset action is taken.

Spam Help

A powerful context sensitive online help is provided. In any part of the screen, click F1 to bring up the help file with the related content.

License Information

This menu allows you to enter the License key. Enter the proper key in the dialog box that is displayed and select **OK**.

Change Password

You can change the password required to operate X-Spam. This ensures that unauthorized people do not change the settings. Enter the old and new passwords in the dialog box and select **OK**.

About

The menu shows a splash screen of X-Spam. Contact information of MicroWorld, creators of X-Spam are displayed along with the X-Spam version number.

Index

A

About MicroWorld, 8
 Acknowledgement Routing by Users, 26
 Acknowledgement & Routing by Users, 26
 Acknowledgment for Non Local User, 26
 After Update, 42
 Allow Client for Authentication, 28
 Allow Connections coming in on any interface, 19
 Allow Relay from ONLY from User/IP, 17
 Anonymous, 42
 Audience, 5
 Authentication, 16, 19, 27, 28
 Authentication IP, 28
 Auto Download is Enabled, 10
 Automatic download of Updates at, 44
 Available Domain List, 23
 Available User List, 28

B

Bind To IP, 19

C

Check if HELO/EHELO domain matches connecting IP, 33
 Check if Mail FROM domain matches connecting IP, 33
 Check if Sender Domain is valid before accepting email, 32, 34
 Classify as non Spam if score is below, 37
 Classify as Spam if score is above, 37
 Contact Us, 7
 Custom, 38, 41

D

Default Scores, 38
 Details, 10
 Details of MailScan tasks, 10
 Dial_Up Users List, 33
 Dial_Up Users List (DUL), 33

Disable MailScan, 10
 DNS Server IP Address, 17
 Do reverse DNS on connecting IP, 33
 Domain Name, 16, 23
 Download Anti Virus Update, 10

E

Edit Local Domain to IP Mapping, 16, 17
 Enable Autodownload, 42
 Enable Download Via Proxy, 42, 44
 Enable Force Authentication, 28
 Enable Mail Size Restriction, 21
 Enable Proxy Authentication, 28
 Enable Routing by User, 26
 Enable Update Notification, 42
 eScan Updater Options, 42
 Execute this, 42

F

Features of X-Spam, 9
 Flush DNS, 17
 Force Process, 42
 Forward to Host, 16
 FTP, 42

G

Gateway Configuration, 14, 15
 General Configuration, 42

H

Heuristic Filter, 12, 14, 15, 34, 50
 Hide All Icons, 42
 How this guide is organized, 5
 HTTP, 42
 HTTP Config, 42
 HTTP Proxy Server IP, 44

I

ID, 42
 Import, 29
 Incoming Enabled, 16
 incremental, 42
 Internet, 42
 Internet to Local, 21
 IP address, 42

IP Addresses of the sites that are exempt from Spam RBL lookups, 33

L

List of Local Domains, 16
 local, 42
 Local to Internet, 21
 Local to Local, 22
 Login name, 42

M

Mail Debug Information, 10
 Mail Delay, 19, 20, 21
 mail parking, 19, 21
 Mail Parking, 20, 21
 Mails for Local Domains, 16
 Mails From Users, 18, 24
 Mails from Users/Domain, 24
 MailScan is Active, 10
 MailScan Tasks, 10
 Maximized, 42
 Maximum Incoming Threads, 18
 Meta Test, 34, 39, 40
 Minimized, 42
 Modify, 38, 39, 40, 42

N

Network, 42
 No. of Connections Per IP, 20
 Normal Windows, 42

O

Our Asia Pacific office, 7
 Our Head Office, 7
 Outgoing Enabled, 16

P

Parameters, 42
 Password, 6, 14, 16, 28, 44, 46, 50
 Port, 42
 Predefined, 38, 40, 41
 Program Name, 42
 protocol, 42
 proxy, 42

R

RBL / DUL Settings, 27, 32
RCPT Limit, 20
Realtime Blackhole List, 32
Realtime Blackhole List (RBL), 32
Regular Expression Tests, 34, 37, 38
Regular Expressions, 9, 34
Reject unauthorized relaying, 17
Replace To, 23
Retry Delays In Minutes, 19
Route To, 24, 25
Run, 42
Run Regular Expression tests off all facts, 37
Run Regular Expression tests till first positive test, 37
Run Regular Expression tests till score crosses threshold, 37

S

Save, 42
Send Acknowledgment, 26
Send Copy To, 24, 25

Send EHLO, 19
Set auto actions after update downloads, 42
Set General Updater Configuration, 42
Set General Updater Configuration, Password, 42
Set update download mode, 42
Sharepoints, 10
SMTP Config, 12, 14, 15, 17, 27
SMTP Controls, 17, 19, 20
SMTP Outgoing, 19
SMTP Server to Listen on Port, 18
SMTP Settings, 17, 18
SMTP Spam – General Configuration, 14, 15, 17
SMTP Spam – Spam Configuration, 14, 15, 27
SMTP Spam Config, 12, 17, 27
Start in, 42
System Information, 10

T

Tarpit Count, 20
Tarpit Delay, 20

To enable updates auto download, 42
To launch MailScan tasks, 10
To set time for updates auto download, 42
Typographical Conventions, 6

U

Update Config, 12, 14, 15, 42
Update notification Mails from user, 42
Update notification Mails to user, 42
Update now, 42
Use this Account as an Authentication, 29
User Name, 16, 28

V

Version Request HTTP, 42

W

Warning When Entering Level, 19
Welcome, 5
White / Black List, 34, 41