MailScan

for Exchange - V8

User Guide

24x7 FREE
Online Technical Support

support@escanav.com
http://forums.escanav.com

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

Current Software Version: 8.x.x

Copyright Notice: Copyright © 2020. All rights reserved.
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 changes without prior notice.
No part of this publication may be copied without the express written permission of MicroWorld.

Trademarks: The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, MailScan are trademarks of MicroWorld.

Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All product names referenced herein are trademarks or registered trademarks of their respective companies. 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 reserves the right to modify specifications cited in this document without prior notice.
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.

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

Technical Support:	support@escanav.com
Sales:	sales@escanav.com
Forums:	http://forums.escanav.com
eScan Wiki:	http://www.escanav.com/wiki
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld
Date:	July 2020

Contents

Introduction 6
Key features of MailScan 7
Minimum system requirement 9
Other requirements 9
Pre-installation Requirement 9
MailScan for Exchange Deployment Scenarios 10
Installing MailScan for Exchange 20
Validating MailScan Installation 27
MailScan Web Console 28
Quick Links 29
SMTP Administrator 31
Gateway Configuration 31
General Configuration 31
Configuration for Inbound Mails 33
Configuration For Outbound Mails 35
User and Mail Restriction 36
Internet 36
Restriction From Users 40
Restriction To Users 42
Spam Control 44
Settings 44
GreyListing 46
User Based Rulesets 47
Mails From User 47
Mails To User 48
Acknowledgement & Routing by Users 49
Authentication 51
Server Settings 53
SMTP Settings 53
SMTP Controls 55
SMTP Proxy 57
ETRN Setting 58
Substitute Domains 59
Policy Replication 60
IP Whitelisting 61
Scanner Admin 62
Forward Attachments 62
Forward Attachments of following Types To Admin 62
Reserved Attachments Check excluded for email To/From 63
Attachment Control 64
Block Attachments types 64
Configuration 65
Attachments Excluded (Whitelist) 65
Action 66

Advanced 66
IE vulnerabilities 66
Archival 69
AV Update Configuration 70
After Update Settings 73
Execute this program, after successful download 73
Content/Spam Control 75
Configuration 75
Advanced 76
Advanced Content Options 77
Anti-Spam Options 77
Mail Tagging Options 78
Disclaimer 79
Advanced 80
Do not send disclaimer for Mails to 80
Domain Specific Disclaimer 80
Antispam Configuration 81
Auto Spam Whitelist 83
Quarantined Mails 84
Compression Control 85
Configuration 85
Attachment Compression 86
DO NOT compress attachments of extensions 87
Mail Attachment Compression 87
MailScan Messages 88
Messages 88
Notifications 90
Outbreak Alert 91
Scan Control 92
Scan Mails Only 92
Do Not Scan Mails 93
Advanced 93
Managed Email Ids 94
Email Id 94
Add New Group 94
Add email IDs to the Group 95
Delete a Group 95
Settings 96
Quick Links 97
Logs 98
View Logs 98
Flush Logs 99
Reports 100
Reports 100
SMTP Reports 101
Report Criteria 102

Generating a Report 102
Report Options 103
Summary Report 104
Email Traffic Report 105
Inbound Connection Report 105
Accepted Mails Reports 106
Associated Reports 106
License Information 108
Check RBL 108
Virus Test Mail 108
Help 109
Additional Tools 110
Preferences 111
User Management 111
Check Authentication 112
Web Console Settings 113
Mail Debug Information 114

Introduction

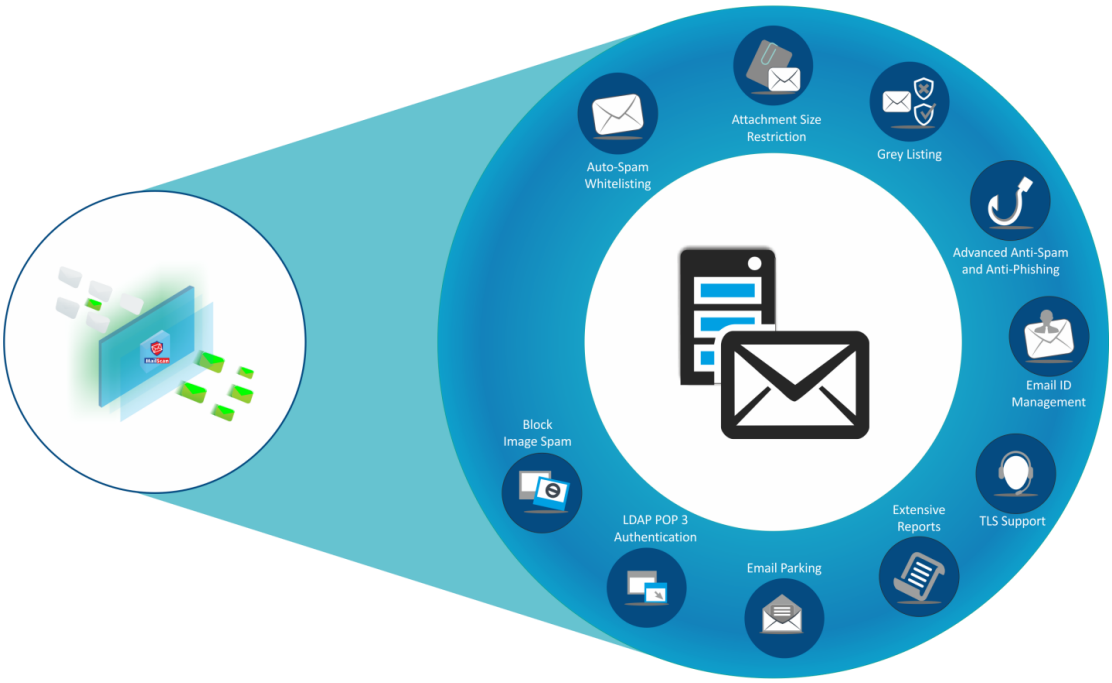
MailScan for Exchange is designed to protect email traffic running Microsoft ® Exchange server from various security threats. It has several advanced features for ensuring the integrity of the email communication in the organization.

Following are the benefits of MailScan for Exchange:

- **Spam filtering:** MailScan checks emails for spam before delivering them to the Information store.
- **Content filtering:** MailScan filters email messages and screens out unwanted content based on the occurrences of specific words or phrases.
- **Attachment blocking:** MailScan allows you to block attachments based on file types or file names.
- **Virus scan:** MailScan detects malware, such as viruses, worms, Trojans, and others in your emails.

You can configure MailScan as a Gateway Server. If you configure it as a gateway server, you can avail the SMTP features. It performs virus scanning, blocking malicious or unwanted attachments, VSAPI scanning, spam filtering, and content scanning.

Key features of MailScan



- **Web Based Administration Console**: Using web-based admin console, MailScan's operations can be accessed and managed from a central location.
- **Integrated Security Policy Enforcement**: MailScan allows you to create policy-based rule sets on a universal or organization specific needs.
- **Advanced Anti-Spam and Anti-Phishing**: MailScan stops spamming and phishing emails using combination of technologies like Non- Intrusive Learning Patterns (NILP), Greylisting, Real-time Black List (RBL), SURBL, General Header Tests, MX/A DNS Record Verification, Reverse DNS, X-Spam Rules Check, Barracuda, spam cop.
- **Real-Time Virus Scanning at the Mail Gateway**: MailScan scans all the emails in real-time for viruses, worms, Trojans, adware, and hidden malicious content using powerful, heuristic driven dual Anti-Virus engines. Thus, online threats are prevented before they enter the network via emails.
- **Blocking Image Spam**: MailScan uses powerful in-built technologies to filter out image spam.
- **Real-Time Content Scanning**: All incoming and outgoing messages are scanned in real-time for offensive words and adult content, with the help of Security Policies.
- **Greylisting**: Mails from unknown senders are temporarily rejected, as most spamming servers do not try to send the same mails again if rejected for the first time. In case, the mail is legitimate, the originating server re-attempts to send the email, which is then accepted.
- **LDAP and POP3 Authentication**: MailScan is powered with LDAP and POP3 authenticated web administration. This authentication is required to restrict unauthorized access to MailScan Console.

- **Non- Intrusive Learning Pattern (NILP)**: The NILP technology is an advanced spam filtering method that has self-learning capabilities and uses an adaptive mechanism to categorize emails-based on the behavioral pattern of the users.
- **Auto-generated Spam Whitelist**: When a local user sends an email to an email address, the system automatically adds that ID to the Spam Whitelist.
- **Attachment Filtering**: Attachments having file extensions such as EXE, COM, CHM, or BAT are blocked from being sent or received through emails.
- **Policy Replication**: MailScan policies can be replicated across multiple servers thus reducing the administrative overhead of making policy changes across all servers manually.
- **Relay Control**: This module prohibits spammers from using your organizations' IP addresses to send spam emails.
- **Comprehensive Attachment and Email Archiving**: There are customizable options to archive emails and attachments flowing in and out of the systems. This feature also helps in comprehensive content auditing.
- **Support for TLS Connection**: Transport Layer Security (TLS), a protocol that encrypts and delivers email securely and helps to prevent eavesdropping and spoofing (message forgery) between email servers. TLS is a standards protocol based on Secure Sockets Layer (SSL). TLS is rapidly being adopted as the standard for secure email. The protocol uses cryptography to provide endpoint authentication and communications' privacy over the internet. TLS is the email equivalent of HTTPS for web communications and has similar strengths and weaknesses.
- **Managing Email Groups**: MailScan for SMTP Server allows you to define groups and put email addresses in created groups and later define permissions and settings for the defined groups.

Minimum system requirement

Your computer must meet the following minimum requirements:

- **Operating Systems Supported**: Windows® 2000 Service Pack 4 and Rollup pack 1, Windows® XP, Windows® Vista®, Windows® 7, Windows® 8, Windows® Server 2000, Windows® Server 2003, Windows® Server 2003 R2, Windows® Server 2008 (Including R2), and Windows® Server 2012, Windows® Server 2016 and Windows® Server 2019.
- **CPU**: 2GHz Intel™ Core™ Duo processor or equivalent.
- **Memory**: 4 GB & above.
- **Disk Space**: 8 GB & above

Other requirements

- **Web Browser**: Microsoft® Internet Explorer 7.0 & above, Latest version of Google Chrome / Mozilla Firefox.
- **Display**: High-color display with a resolution of 640x480 pixels or higher recommended).
- **Disk Space**: 10 GB (for handling outgoing email queue and database)

Pre-installation Requirement

For first time installation

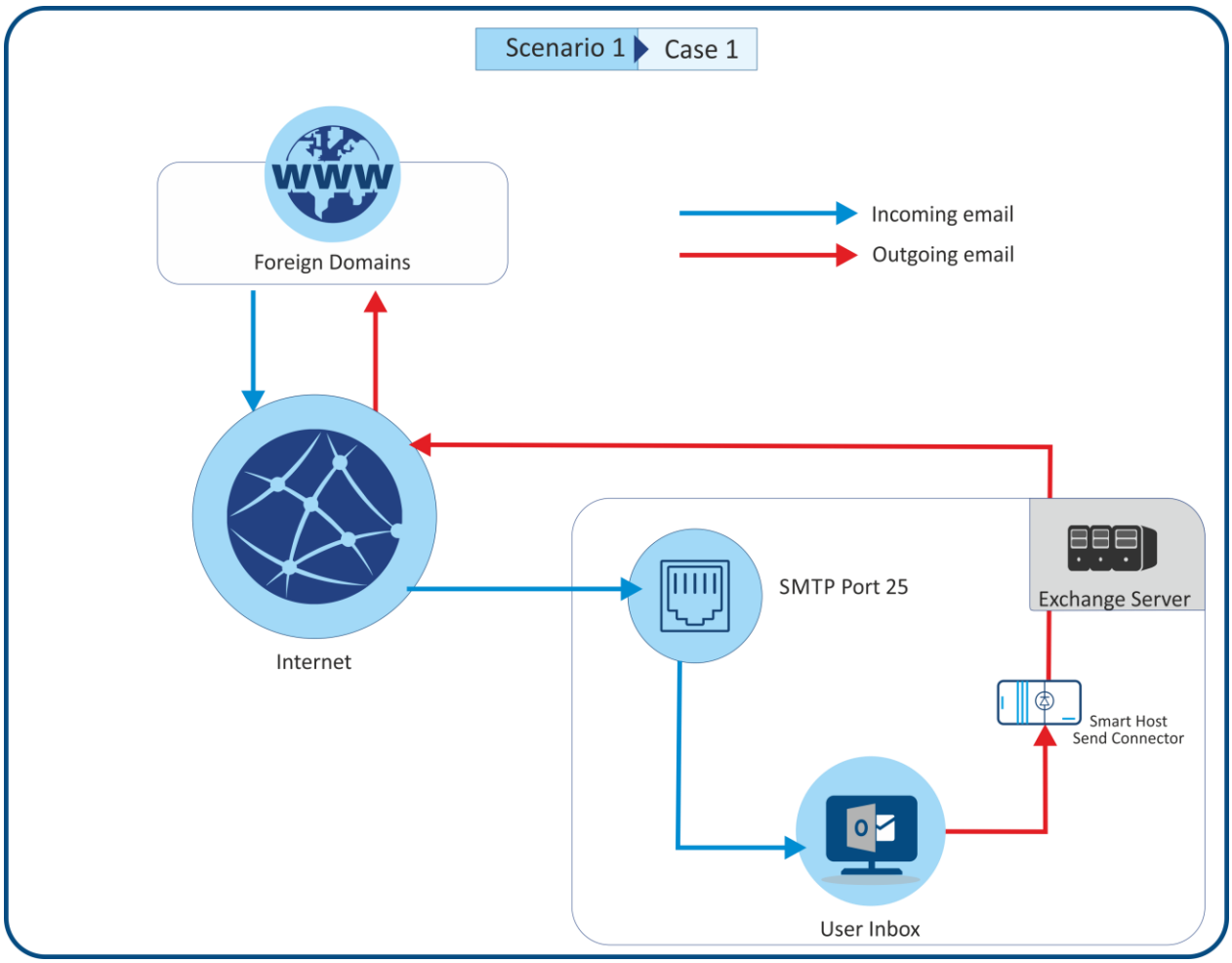
- Ensure that you have administrator rights or equivalent privileges for the user logged on to the computer.
- Install MailScan on the Drive that has sufficient free space.
- It is recommended that the computer on which MailScan is being installed is connected to the internet during the installation process. This will ensure that MailScan downloads all the latest updates from MicroWorld update servers.
- Ensure that the critical operating system and security patches are installed on the computer.

MailScan for Exchange Deployment Scenarios

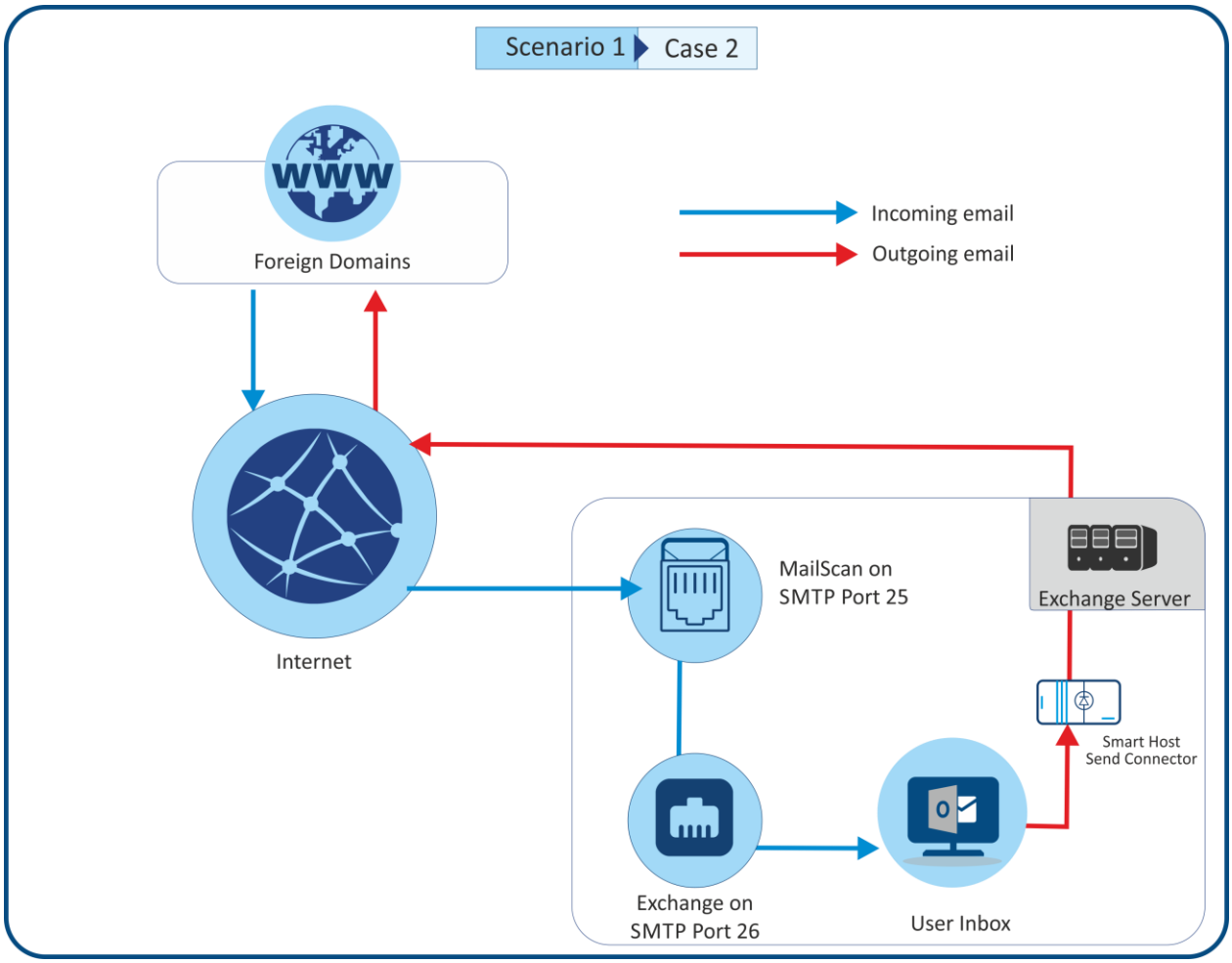
MailScan scenarios for emails received from or sent to Foreign Domains:
Scenario 1 – Company has its own mail server.

Administrator can configure setting in MailScan to scan email received from foreign domains as per requirement.

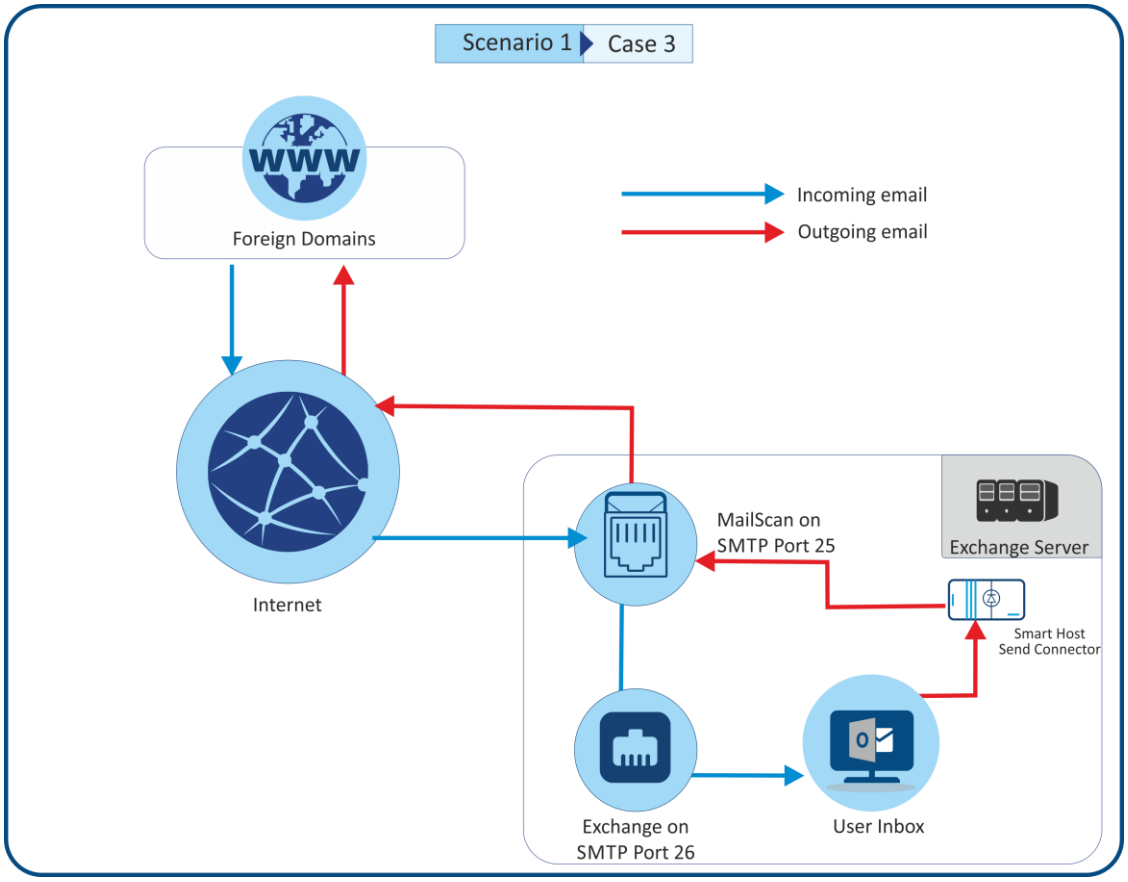
- **Case 1**: Mails received from or sent to foreign domains will not pass through MailScan hence will not be scanned for malware infection.



- **Case 2**: Mails received from foreign domains will be received by MailScan on port 25 and will be scanned malware infection as well as cleaned by MailScan before reaching user inbox, but mails sent by user to foreign domain will not pass through MailScan and hence will not be scanned for malware infection.

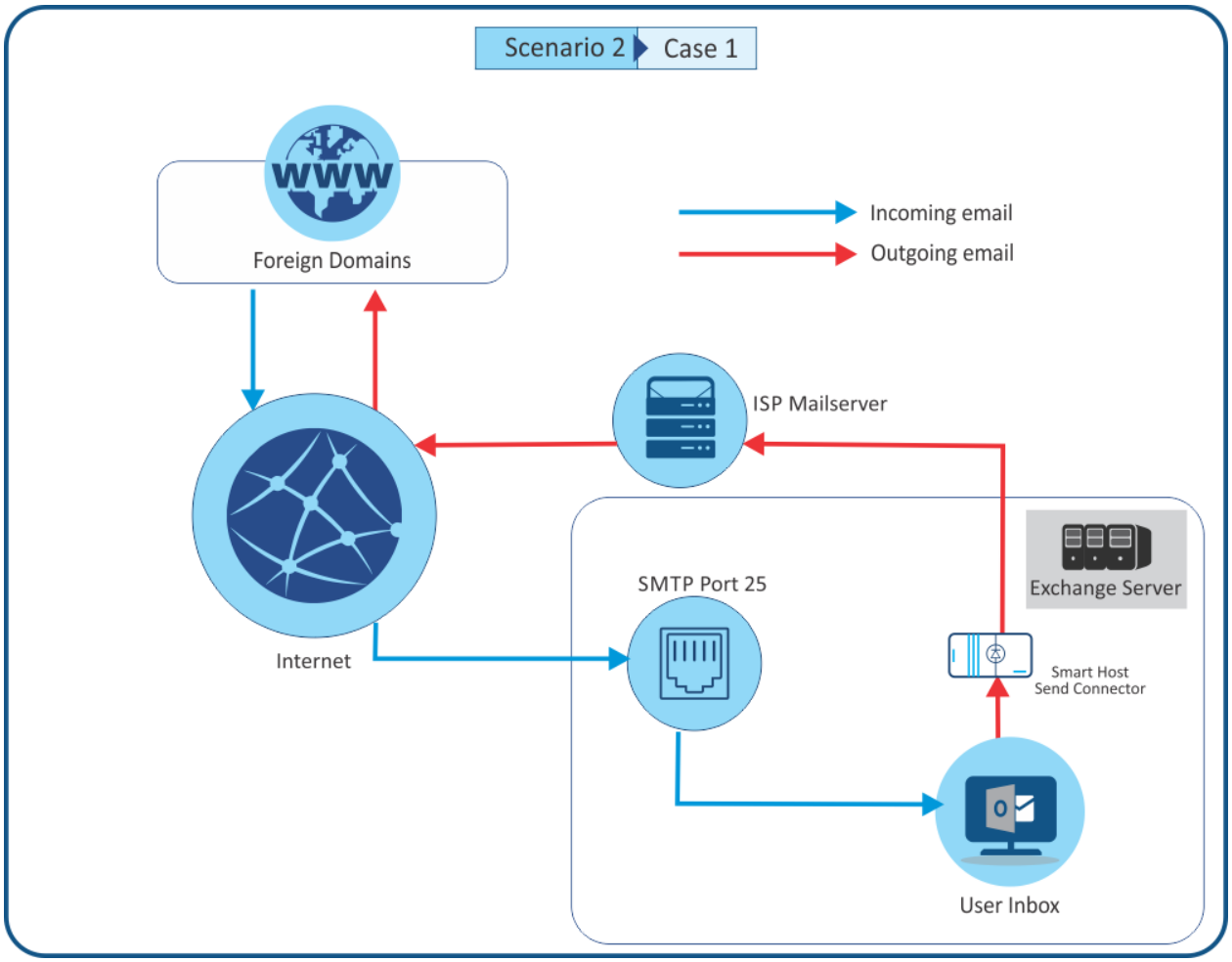


- **Case 3**: Mails received from as well as sent to foreign domains will be scanned by MailScan for malware infection.

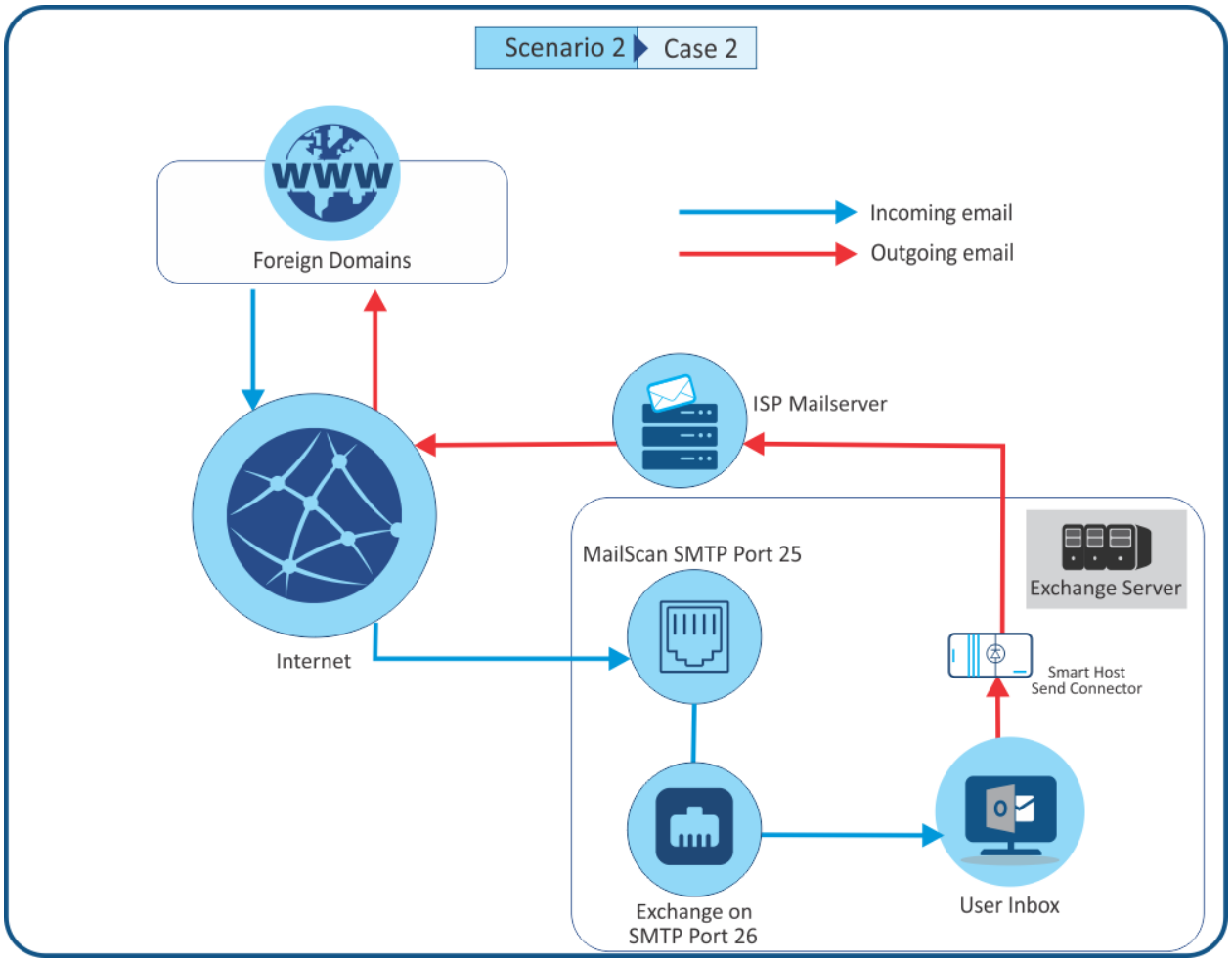


Scenario 2 – External ISP Email Service used.

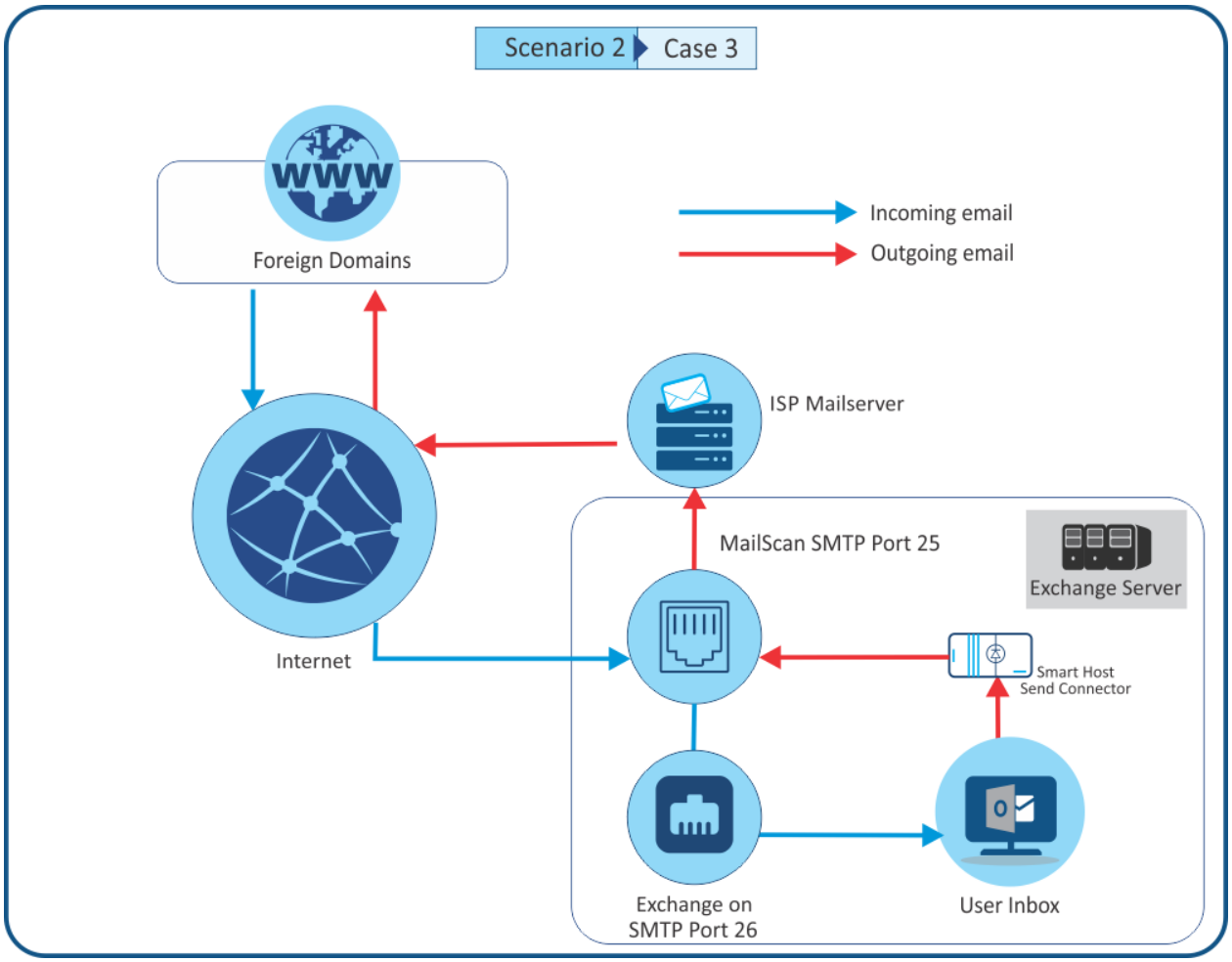
- **Case 1**: Mails received from or sent to foreign domains will not pass through MailScan hence will not be scanned for malware infection. All sent mails from internal domains will be sent to ISPs mail server by Exchange Server.



- **Case 2**: Mails received from foreign domains will be received by MailScan on port 25 and will be scanned malware infection by MailScan before reaching user inbox, but mails sent by user to foreign domain will not pass through MailScan and hence will not be scanned for malware infection. These mails will be directly sent to ISPs mail server that will further push it to external domain.

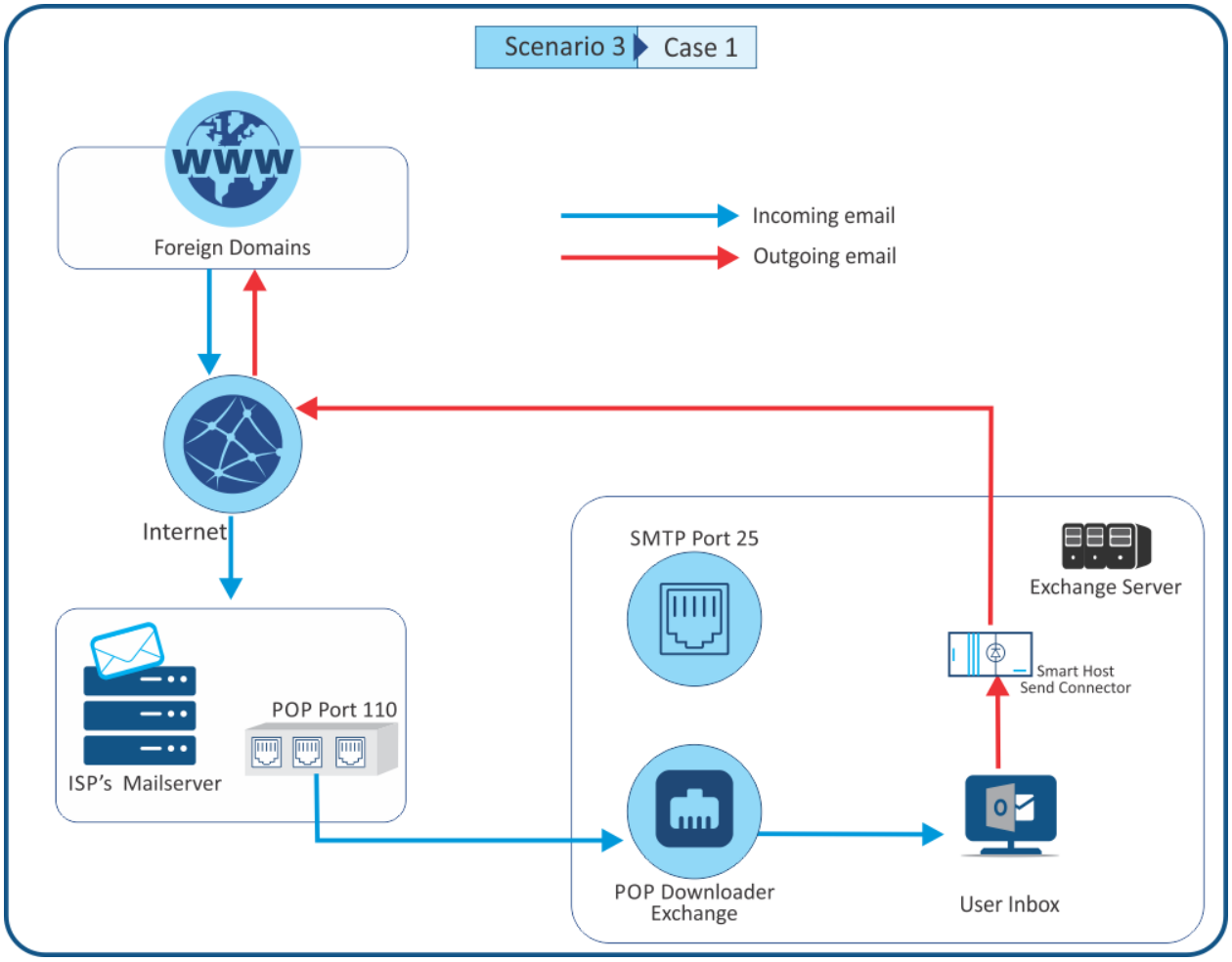


- **Case 3**: Mails received from as well as sent to foreign domains will be scanned by MailScan for malware infection. All sent mails will be scanned by MailScan and then sent to ISPs Mail Server.

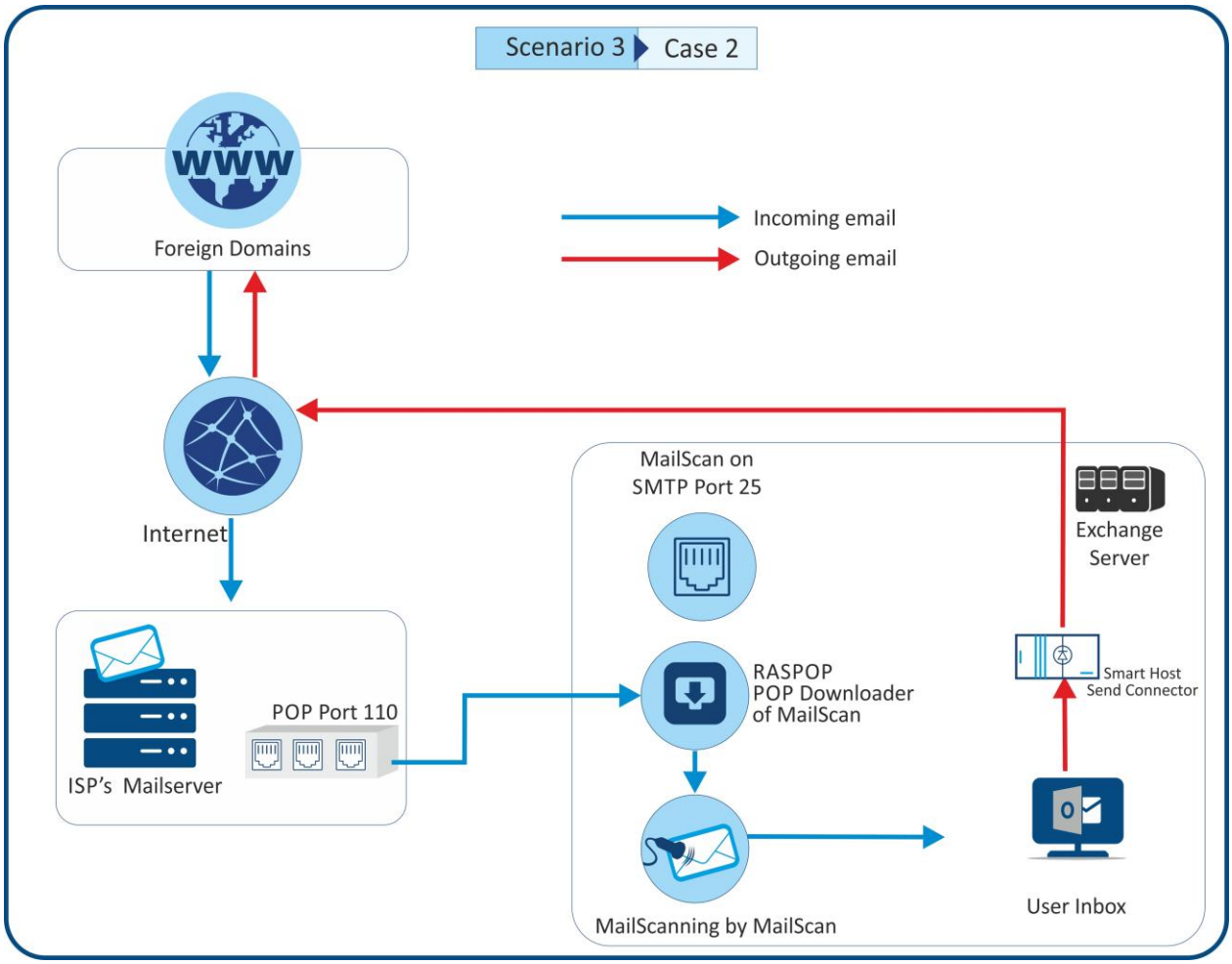


Scenario 3 - Company uses POP3 Email System

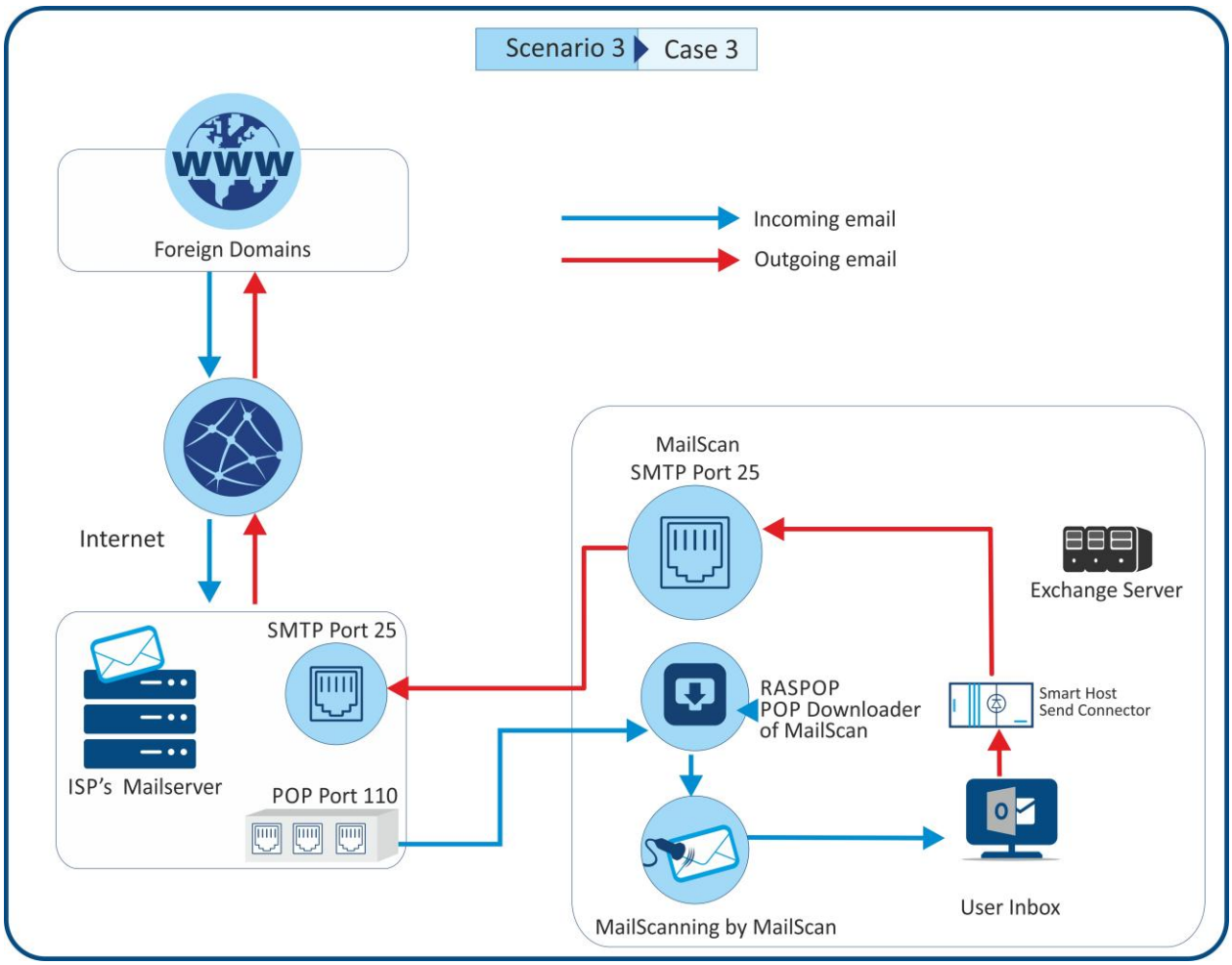
- **Case 1**: All mails received from foreign domains will be forwarded by ISPs Mail Server to POP Downloader of Exchange Server (Third Party POP Downloader) without passing through MailScan hence the mails received will not be scanned for any kind of malware infection. Similarly all mails will be sent by users to external domains will be sent through exchange directly without passing through MailScan.



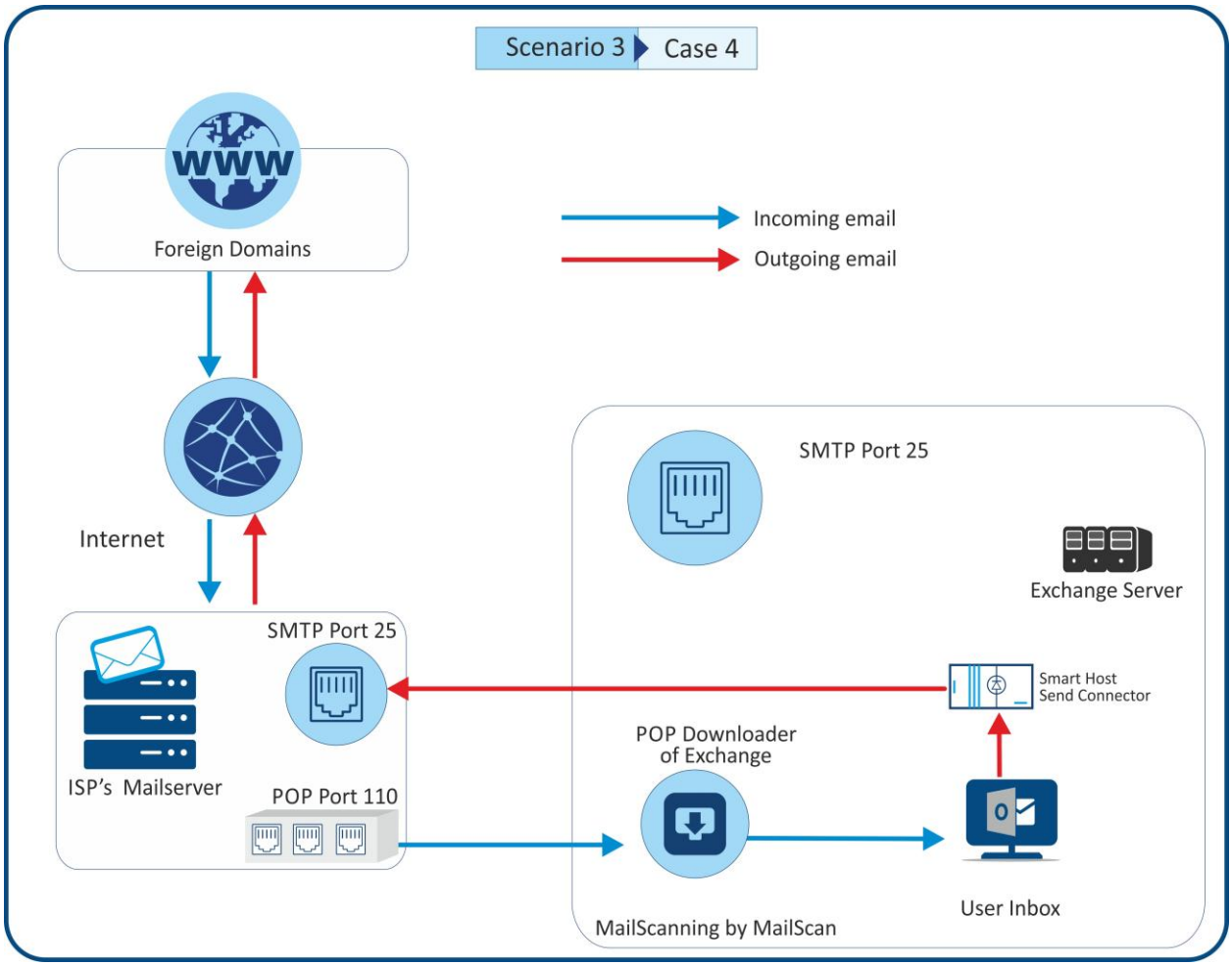
- **Case 2**: All mails received from foreign domains will be forwarded by ISPs Mail Server to RASPOP POP downloader of MailScan which will then be scanned for Malware infection before being delivered to user inboxes. All mails sent by users to foreign domains will be sent directly to the internet without passing through MailScan; hence no scanning will take place for the mails sent to foreign domains.



- **Case 3**: All mails received from foreign domains will be forwarded by ISPs Mail Server to RASPOP POP downloader of MailScan which will then be scanned for Malware infection before being delivered to user inboxes. All mails sent by users to foreign domains will again be sent to MailScan for malware scanning, after scanning these mails will be sent to ISPs mail server which will further forward to foreign domain.



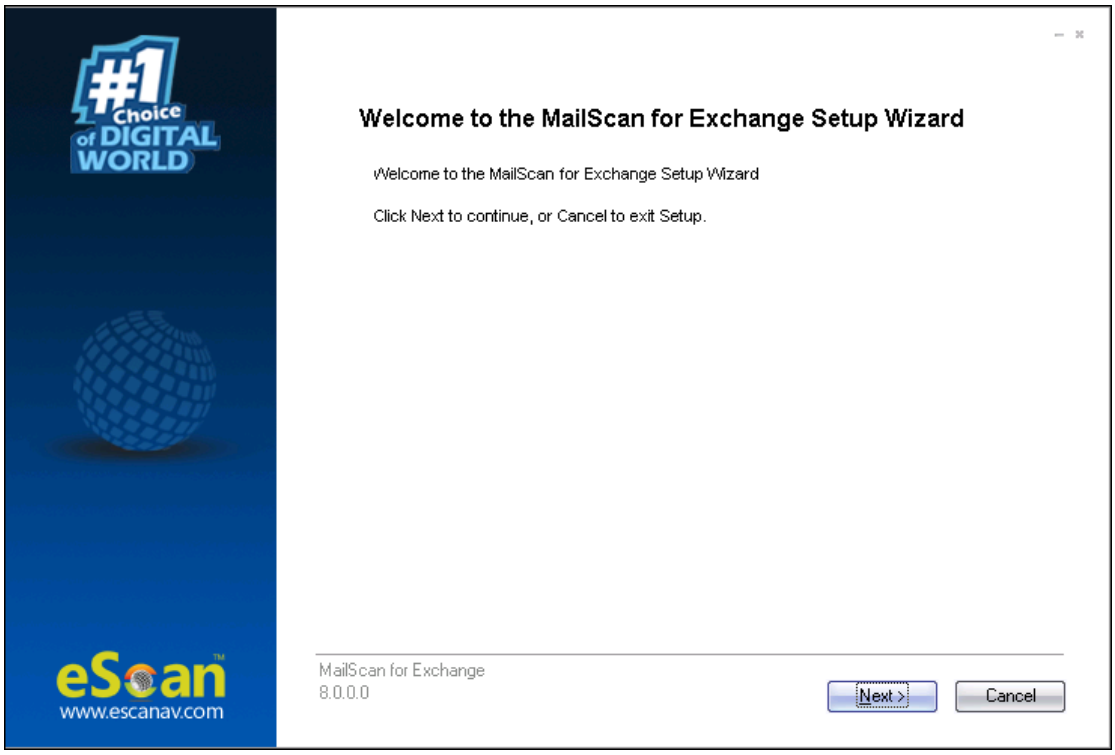
- **Case 4**: All mails received from foreign domains will be forwarded by ISPs Mail Server to POP downloader of Exchange server before being delivered to user inbox. All mails sent by user to foreign domains will be forwarded to ISPs mail server which will further send it to foreign domain. All these mails will not be scanned by MailScan.



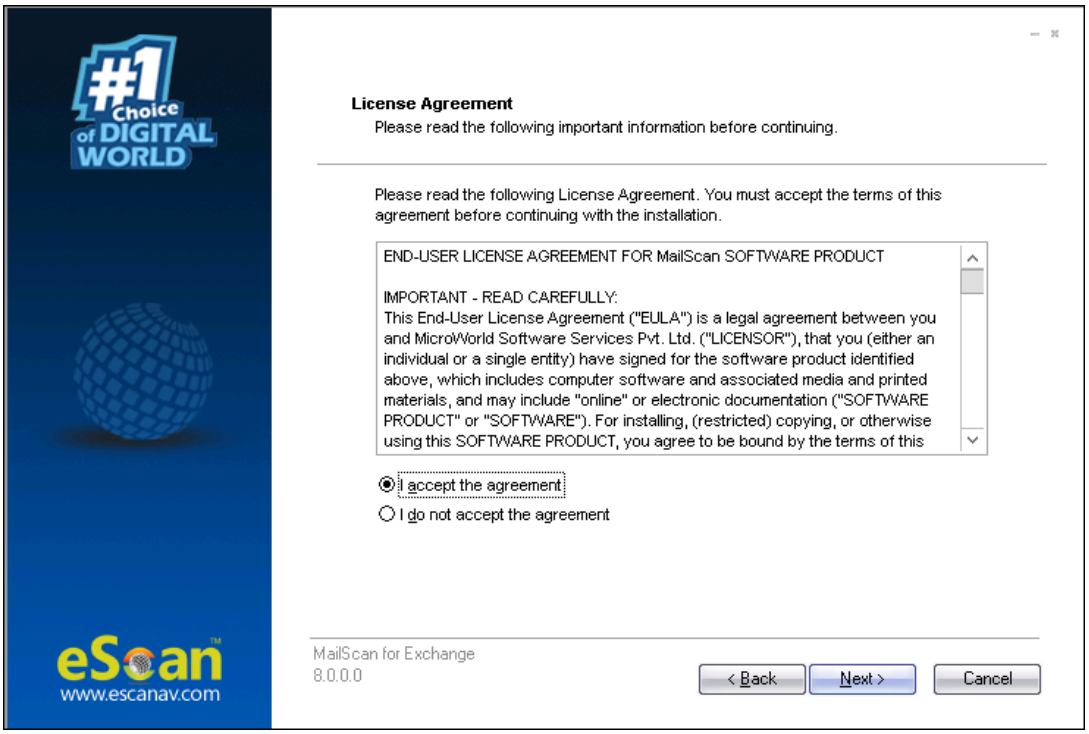
Installing MailScan for Exchange

Use the following simple steps to install MailScan for Exchange server:

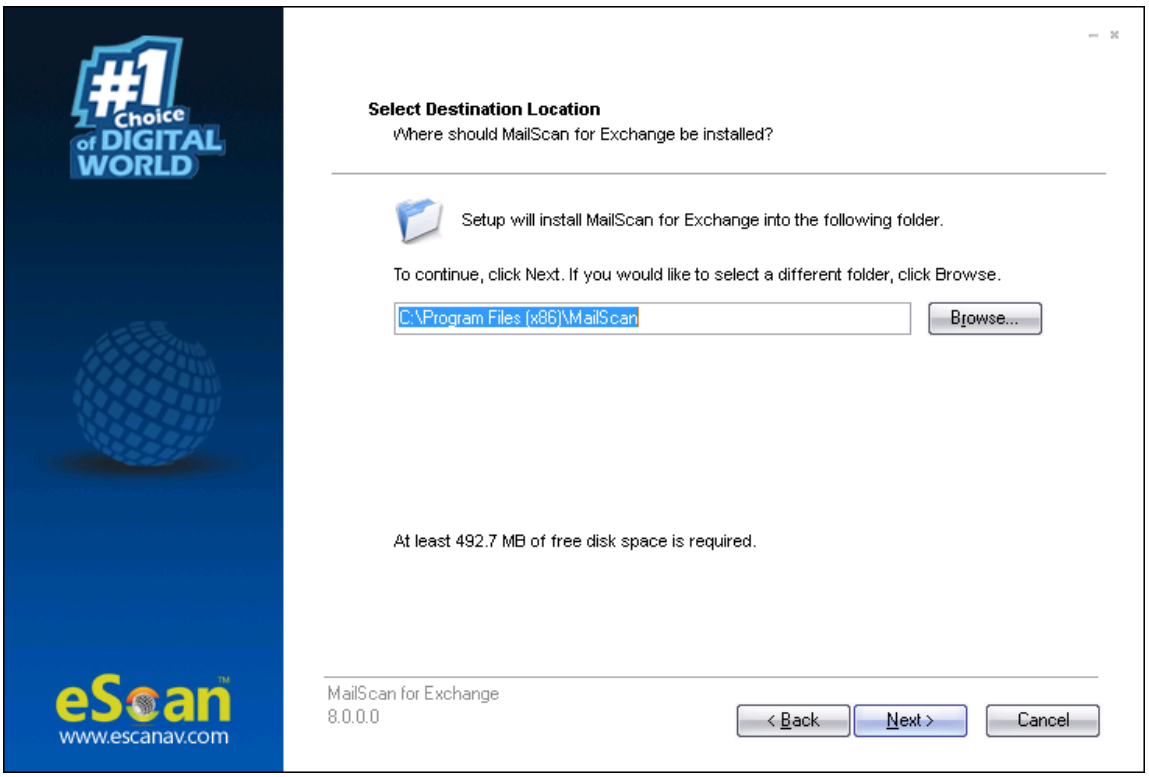
1. Double click on the setup file MailScan for Exchange "**ms2x800a.exe**". This will open the installation Wizard for MailScan for Exchange Installation.



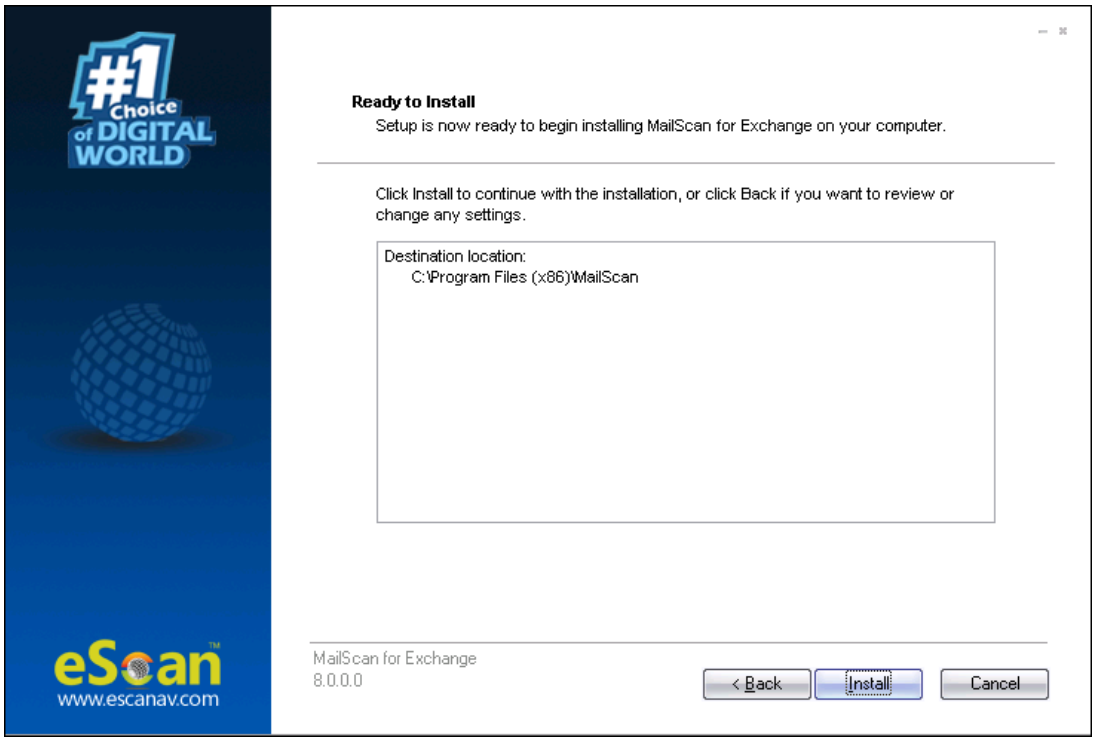
2. Click **Next**> button to proceed with the installation process; License Agreement window appears.



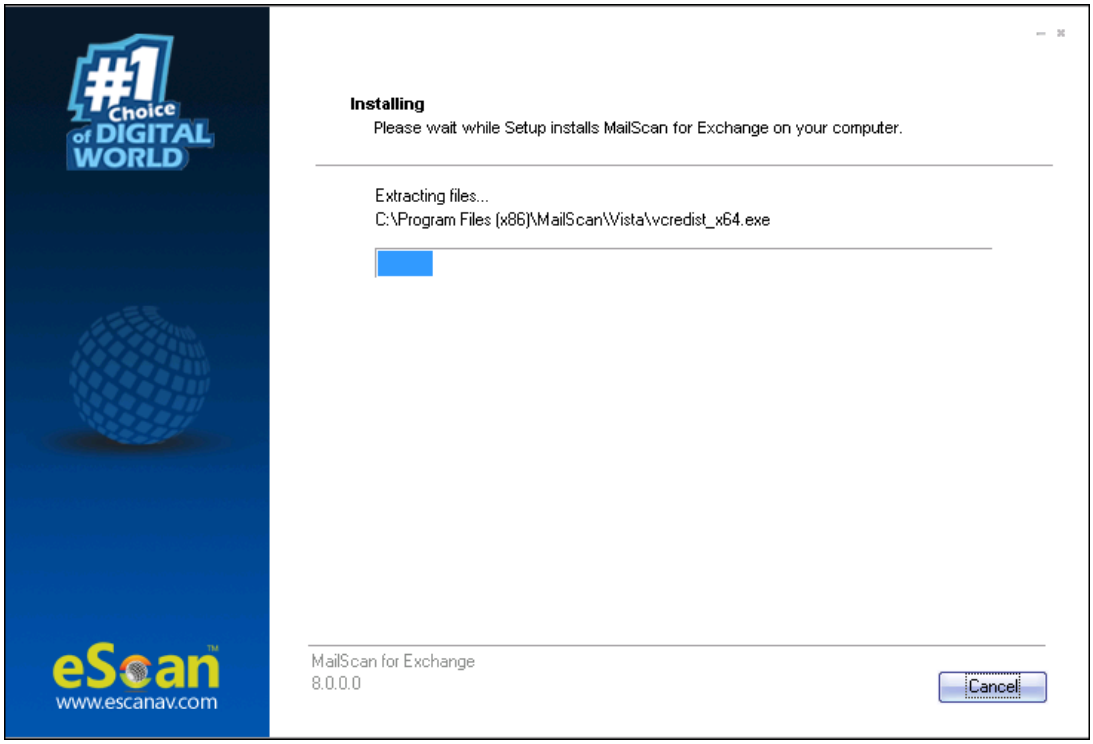
3. Click **I accept the agreement** radio button and click **Next**> button present at the bottom of the interface. Select Destination Folder Window appears.



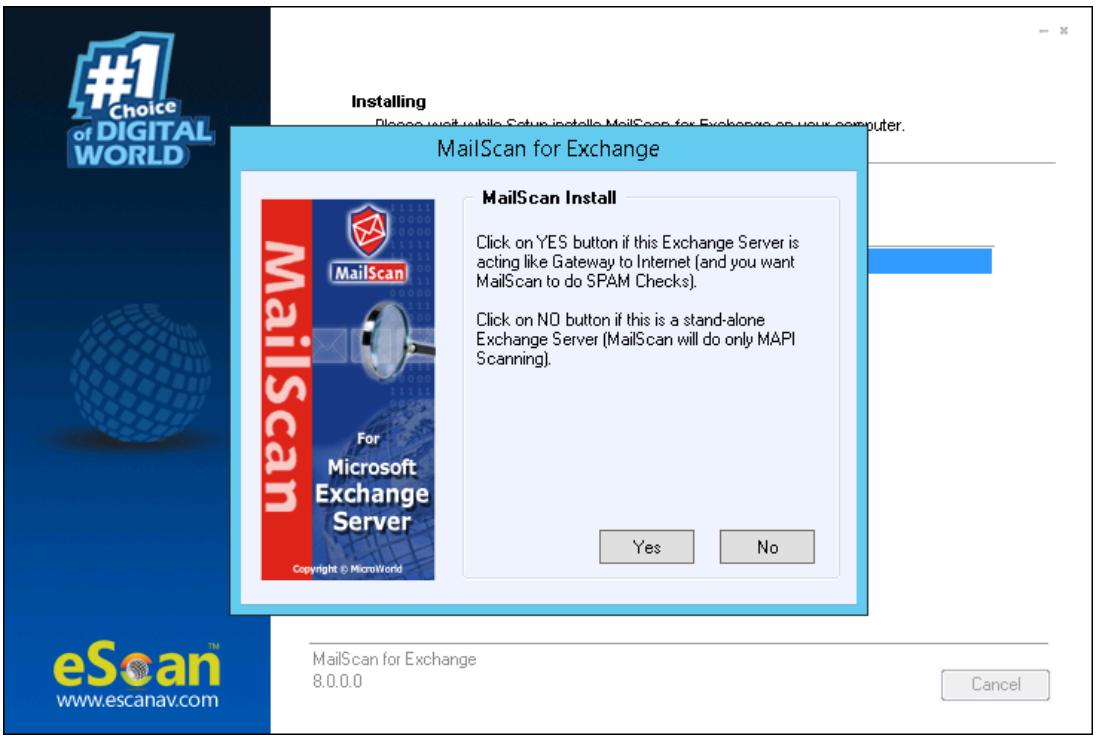
4. Browse the Path/Folder where you wish to install MailScan for Exchange. Click **Next**> button.
5. You will be forwarded to **Ready to Install** window.



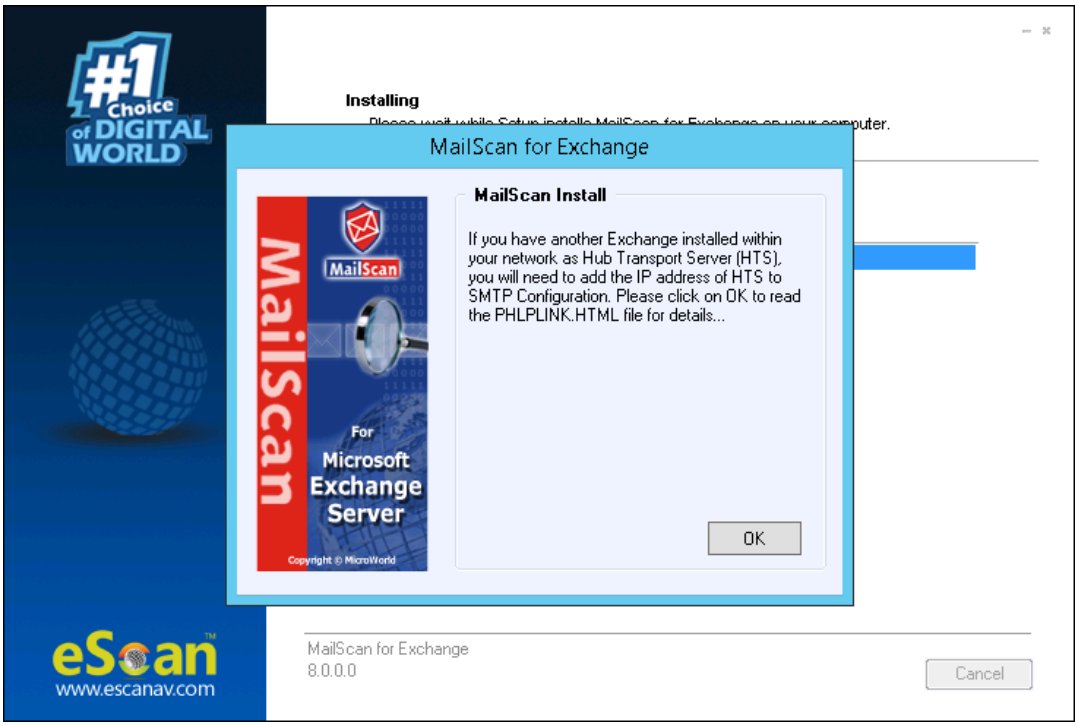
6. Click **Install**. This will start the installation of **MailScan for Exchange** on the system.



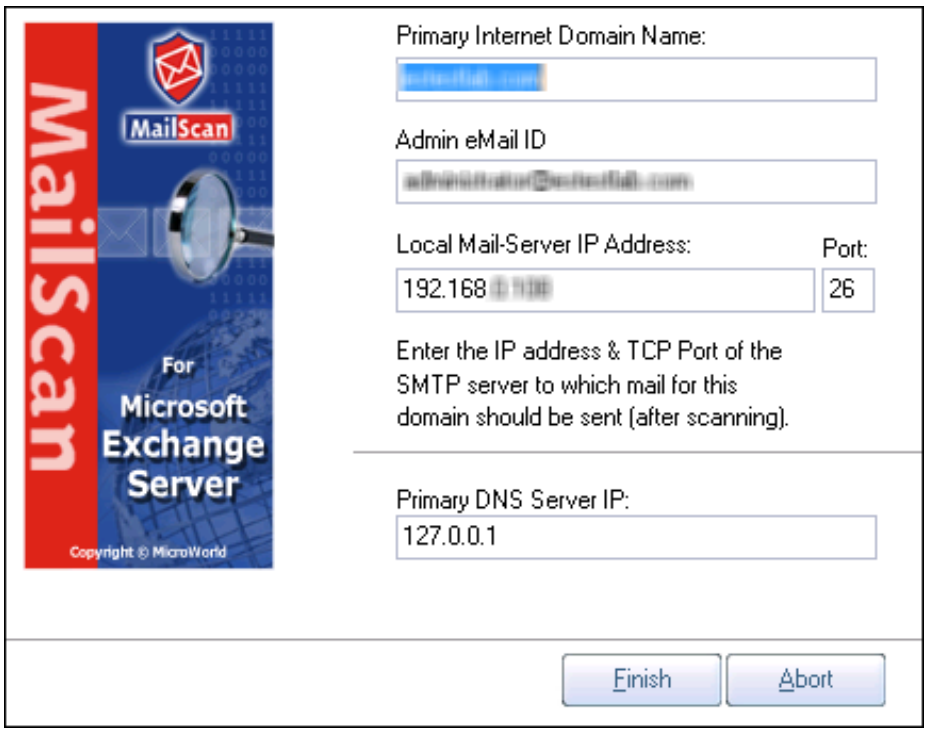
7. During the installation you will be prompted with the dialogue box.



8. Click **Yes**, if this Exchange server is acting as a gateway to the Internet and you want MailScan to check for spam and offensive or malicious content in emails. You will be forwarded to another prompt message. Otherwise, if your Exchange server is a stand-alone email server, click **No**. In this case, MailScan will perform only MAPI scanning.



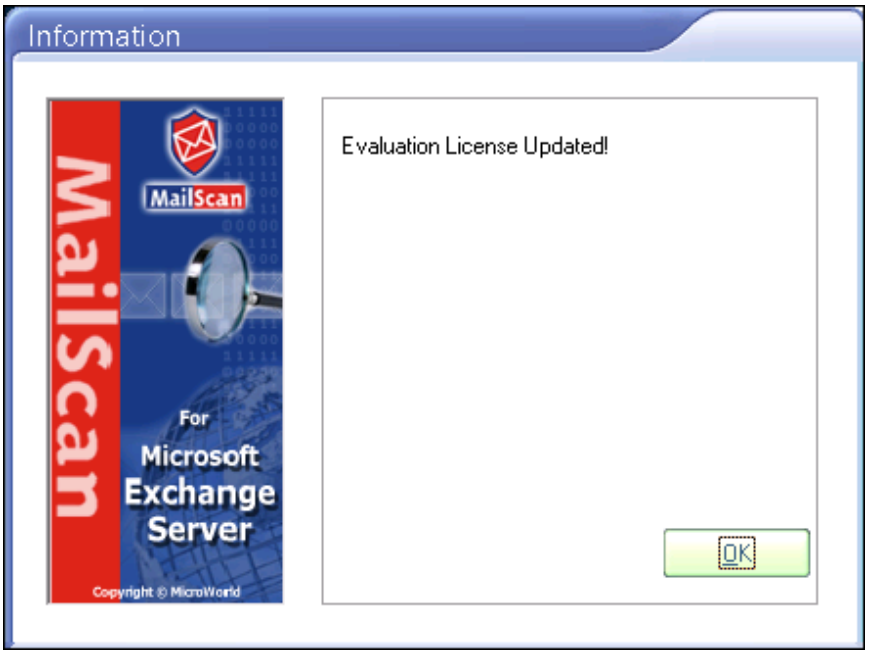
9. Click on **OK** button, you will be forwarded to the following window.



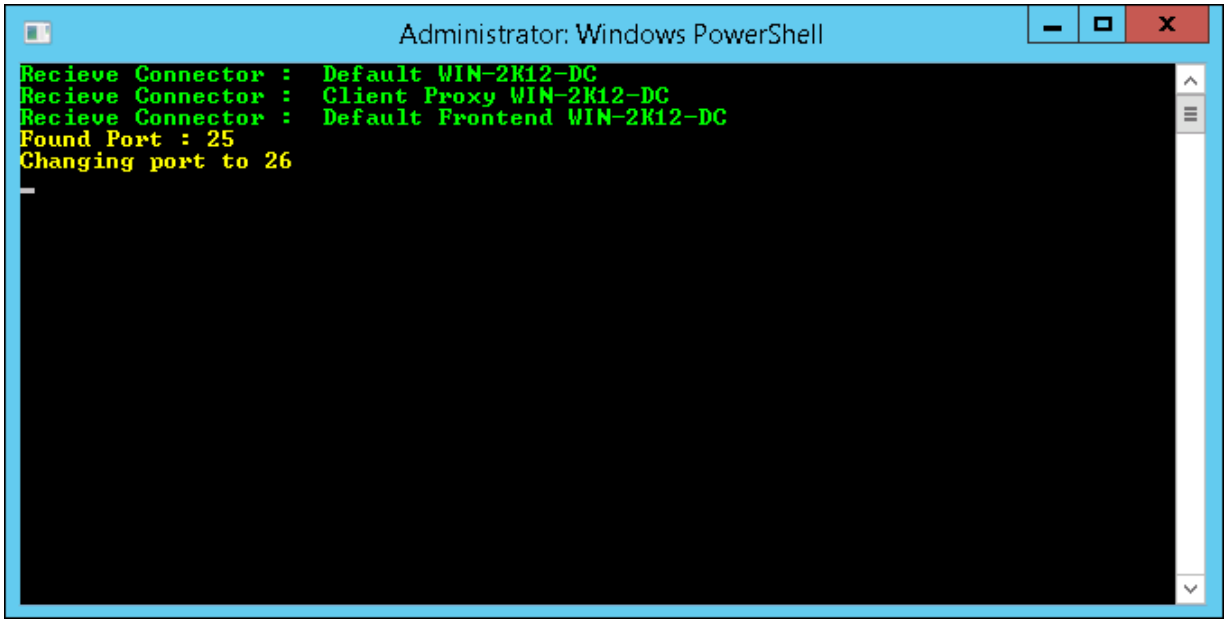
Provide following mandatory details:

- **Primary Internet Domain Name**: Enter the Domain name used for sending and receiving emails such as yourcompany.com.
- **Admin eMail ID**: Enter the email address to which all notification or warning messages will be sent by MailScan.
- **Local Mail server IP Address**: Enter the IP Address and Port number of the mail server to which mail for this domain will be sent.
- **Primary DNS Server IP**: Enter IP address of the Primary DNS Server.

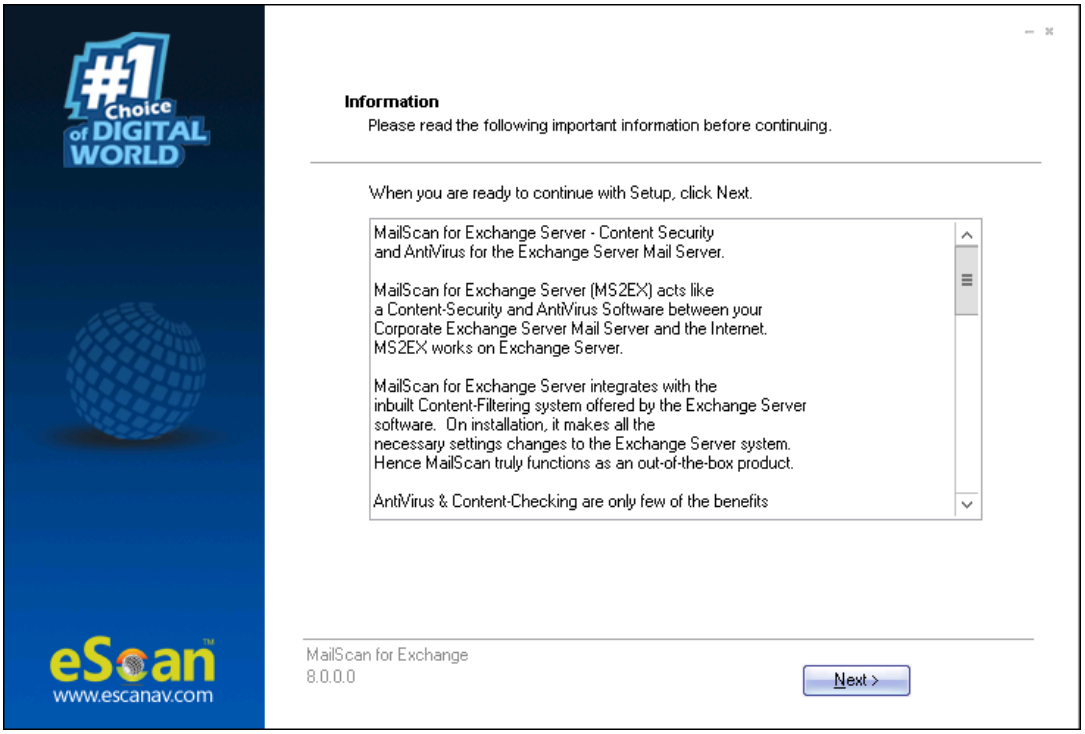
10. Fill in the required above details and click on **Finish** button, this will update your Evaluation period for your License and you will be informed through following message.



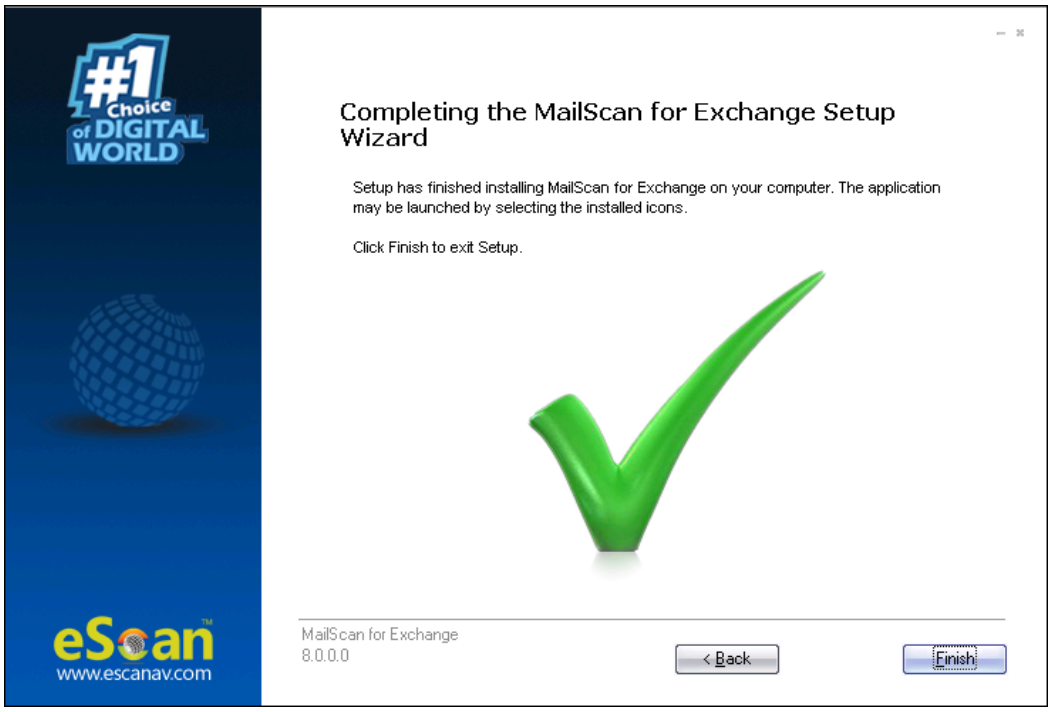
11. Click on **OK** button. This will then automatically set the Microsoft Exchange SMTP port to 26. You will get the confirmation for the same on the Windows PowerShell.



12. After the port change task is completed automatically, following screen is displayed.



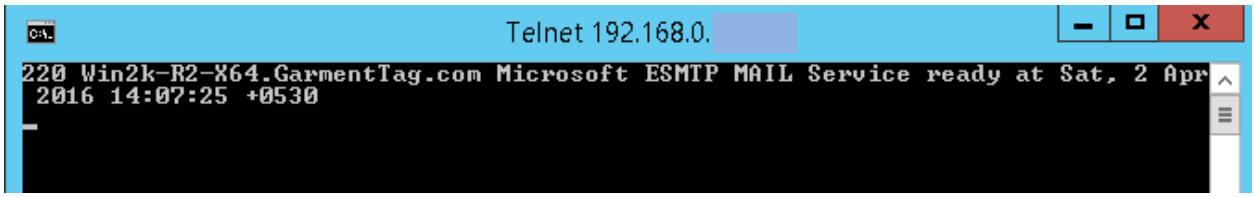
13. Click **Next**>, you will be forwarded to the screen displaying **Completing the MailScan for Exchange Setup Wizard**.



14. Click **Finish** to complete the installation.

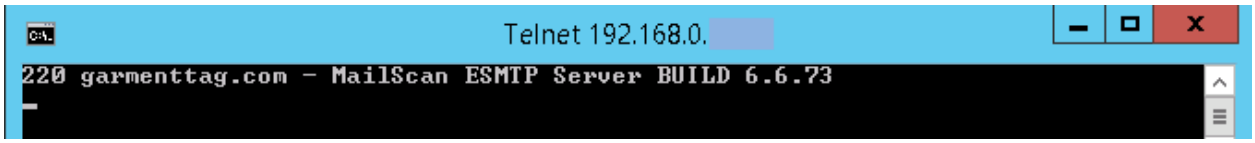
Validating MailScan Installation

1. Click on **Start** and then click **Run**.
2. In the **Run** dialog box, type **cmd** and the press *Enter*.
3. In the Command Prompt window, type **telnet <ip addres> 26.** Press *Enter*.
4. You should get a response from Exchange's SMTP that it is listening.



Note	If you do not get any response, please ensure that the SMTP port is not bound to any IP address. If you need to bind the port to an IP address, ensure that you have specified the correct IP address.

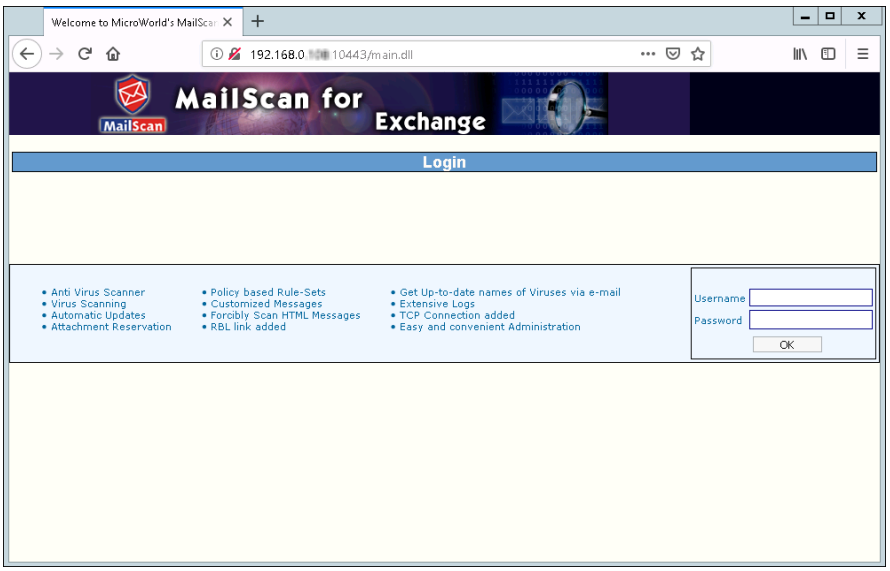
5. Next, in the Command Prompt window, type **telnet <ip address> 25** and then press *Enter*.



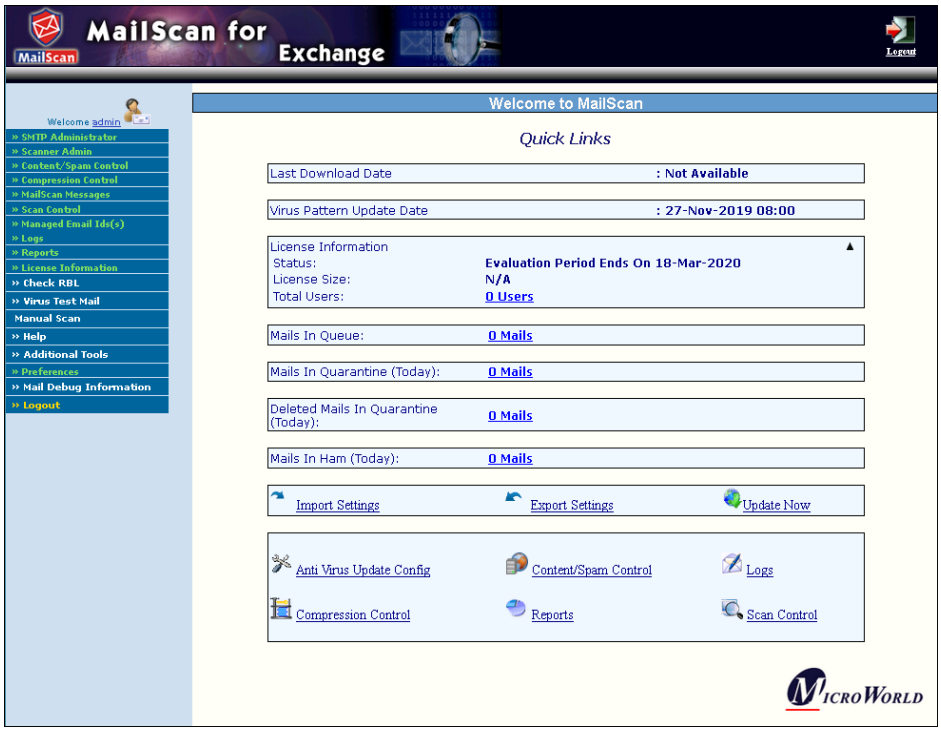
MailScan Web Console

To login to the MailScan Web Console, perform the following steps:

1. Launch the browser.
2. Enter the following URL
   https://<IP address of the installed system>:10443.
3. MailScan for Exchange login page appears.

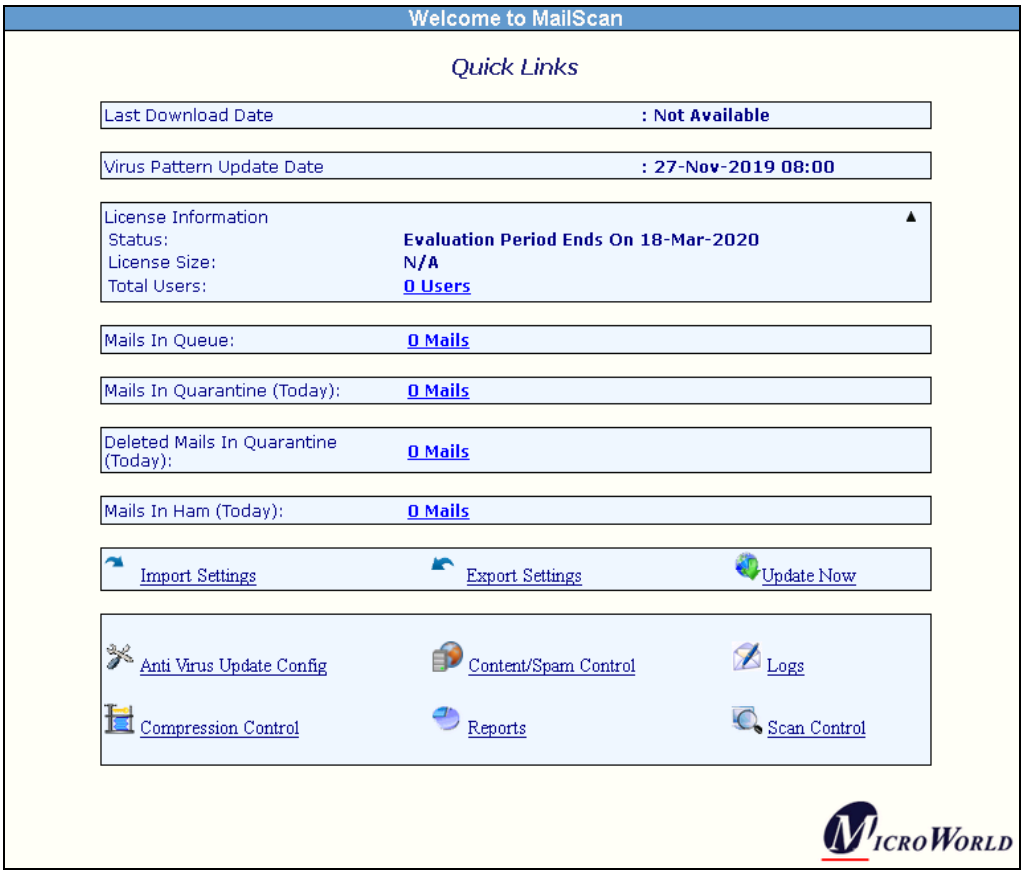


4. Enter the default username "admin" and password set during installation, and click **OK**. Welcome screen will be displayed.



Quick Links

When you login to MailScan, **Quick Links** are displayed on the right-side in the browser.



This page provides quick overview of the following options:

- **Last Download Date**: Displays the download date for last MailScan update along with time stamp.
- **Virus Pattern Update Date**: Displays the download date of last virus pattern (signature) update along with time stamp.
- **License Information**: It displays Information about the License such as **Status**, **License Size**, and **Total Users**.
- **Mails In Queue**: Displays the number of mails that are in queue for delivery to recipient domain server.
- **Mails In Quarantine (Today)**: Displays the total number of mails that are marked as Quarantine during the day. To learn more, click **here**.
- **Deleted Mails In Quarantine (Today)**: Displays the total number of mails that are marked as Quarantine and deleted thereafter during the day.
- **Mails In Ham (Today)**: It displays the total number of Ham Mails during the day. Ham mails are copy of genuine mails from foreign domain that were delivered successfully to your Microsoft Exchange server.

Additionally, it also provides options to perform following settings:

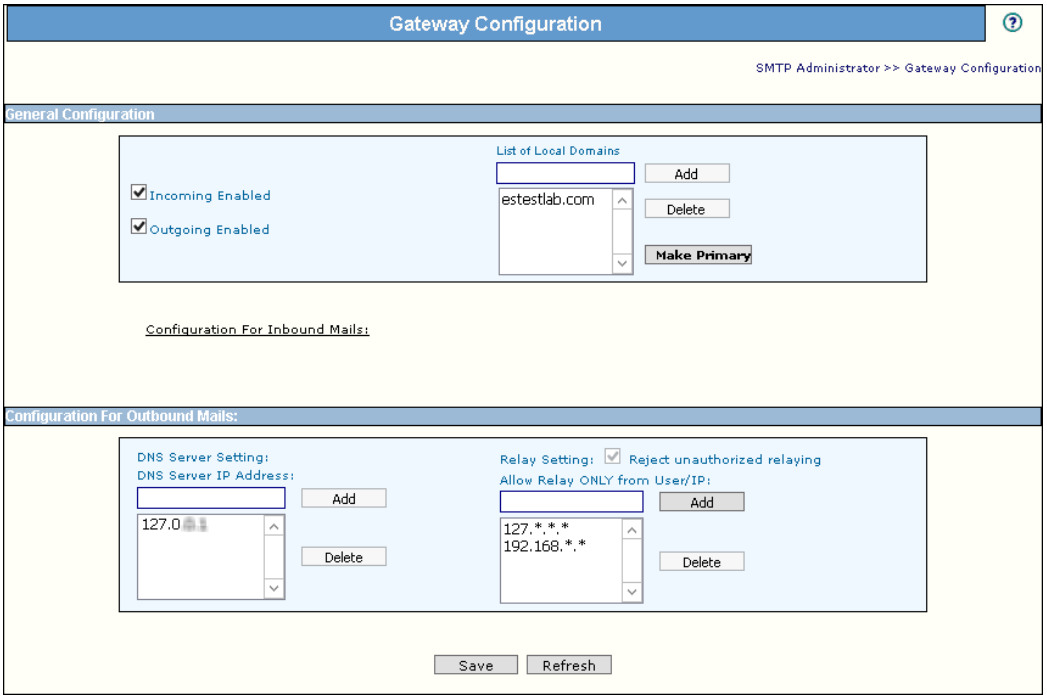
- **Import Settings**: This setting allows to import MailScan settings. You can use this option if you have previously exported MailScan settings and you want to revert to same settings. This option is also useful, in case you have installed MailScan on a fresh computer.
- **Export Settings**: This setting allows to export MailScan settings. In case, in future you install MailScan on a fresh computer, and you want to import the settings using Import option. Then, this option is beneficial in such cases, which will therefore save lot of time configuring all settings again manually.
- **Update Now**: This option allows to manually download latest virus pattern update from internet.
- **Anti Virus Update Config**: This option allows to configure settings for Anti-virus update patches. Learn more about AV Update Configuration, by clicking **here**.
- **Content Spam Control**: This option allows to configure settings for Content Scanning and Spam Control. Learn more about Content/Spam Control by clicking **here**.
- **Logs**: This option is used to View Logs maintained by MailScan on daily basis. Learn more about Logs by clicking **here**.
- **Compression Control**: This option allows to configure settings for compressing email attachments inbound as well as outbound that passes through MailScan. Learn more about Configuration by clicking **here**.
- **Reports**: This option allows to view daily reports of Mail Scanning activity through MailScan. Learn more about this section by clicking **here**.
- **Scan Control**: This option allows to define scan control settings for the inboxes that MailScan is securing. Learn more about Scan Control by clicking **here**.

SMTP Administrator

This module helps you to configure the SMTP server with following submodules.

Gateway Configuration

This submodule lets you configure settings for Inbound and Outbound Mail Traffic. You can also define settings for Host and Domain services.



General Configuration

Incoming Enabled

Selecting this checkbox enables SMTP server to receive emails.

Outgoing Enabled

Selecting this checkbox enables SMTP server to send emails.

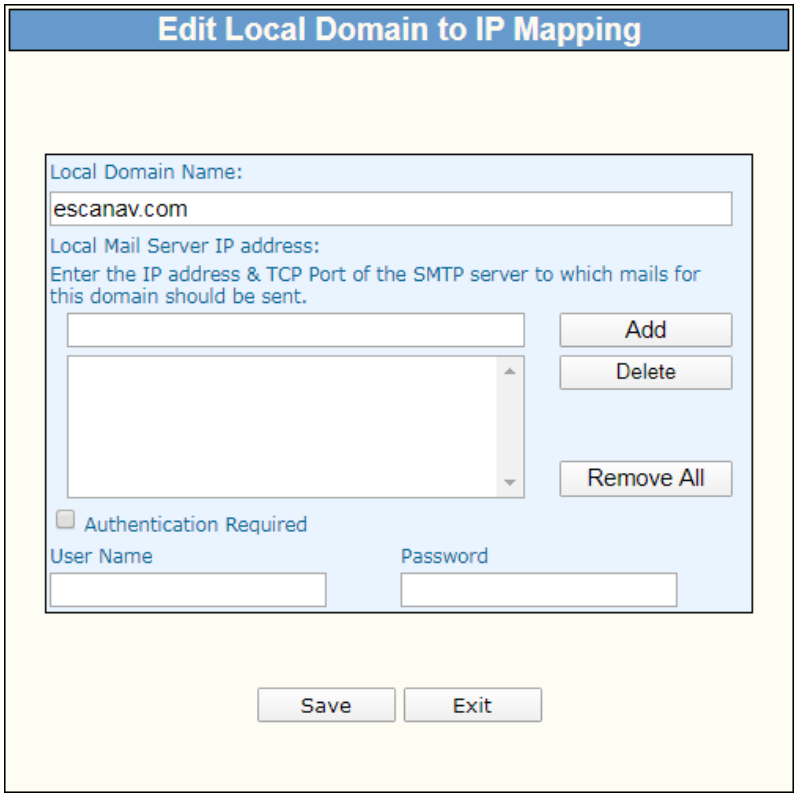
Note	By default, Incoming and Outgoing options are enabled.

The General Configuration also lets you specify local domain names for the Mail Server.

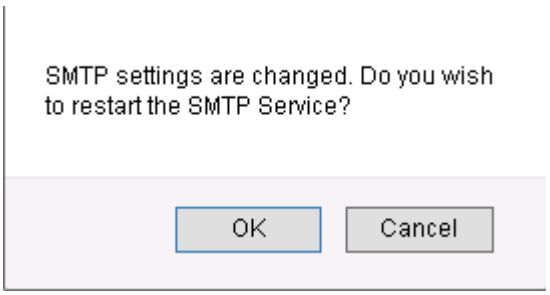
Adding a local domain

To add a local domain, follow the steps given below:

1. Under General Configuration section, enter the local domain name in the **List of Local Domains** textbox.
2. Click **Add**. **Edit Local Domain to IP Mapping** window appears.



3. Enter the **Local Mail Server IP address** and **TCP Port** of the SMTP server. For example, IP address: port number (000.000.0.00:26).
4. If the SMTP server requires authentication, then select the **Authentication Required** checkbox and enter SMTP credentials.
5. Click **Save**. You will be prompted with the following message to restart the SMTP Service.



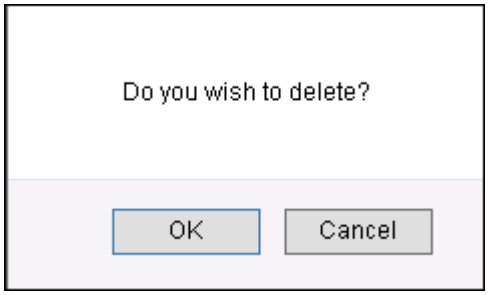
6. Click on **OK**, as the changes will be applied only after the SMTP service is restarted.
7. The Domain Name will be added instantly to the list.

Note	In case of multiple domain names added to the list you can select and make desired domain name as Primary for send and receiving the mails by Selecting the desired domain name and clicking on **Make Primary** button present on the interface.

Deleting a local domain

To delete a local domain, follow the steps given below:

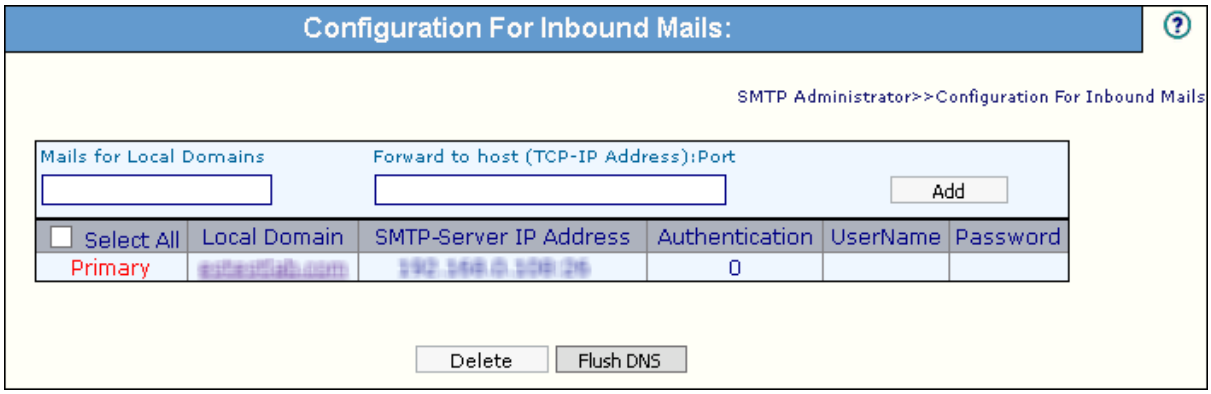
1. Under General Configuration section, in the List of Local Domains, select a domain.
2. Click **Delete**. A confirmation prompt appears.



3. Click **OK**. The domain gets deleted.

Configuration for Inbound Mails

The list box contains information about the local domain, SMTP server's IP address, Port number used by the local domain to connect to the SMTP server, and the authentication details required by the SMTP server, if any.



Adding a local domain and server

To add a server, follow the steps given below:

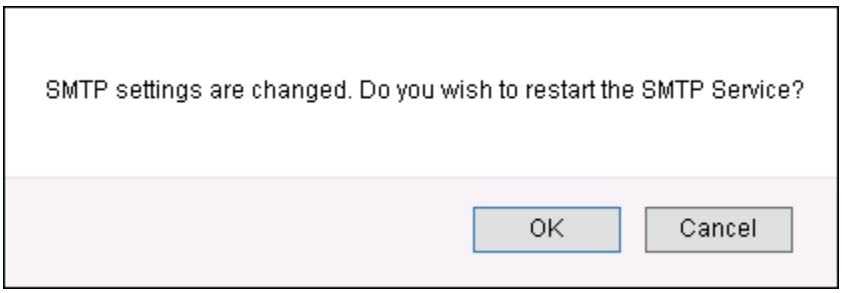
1. In the **Mails for Local Domains** box, enter the local domain names managed by the SMTP server.
2. In the **Forward to Host (TCP-IP address): Port**, enter the SMTP server's IP address.
   All local domains will connect to the SMTP server through this IP address.
   For example, IP address: port number (000.000.0.00:26).
3. After entering all the above details, click **Add**.
   The local server gets added.

Deleting a local domain and server

To delete, select a local server and then click **Delete**.
The local server gets deleted.

Flush DNS

When an email is sent to other domains, the SMTP server finds information like IP address and Port numbers of the remote domains. This information is stored in the registry before mails are sent. To flush the dynamically resolved connections to the remote SMTP servers, click **Flush DNS**.

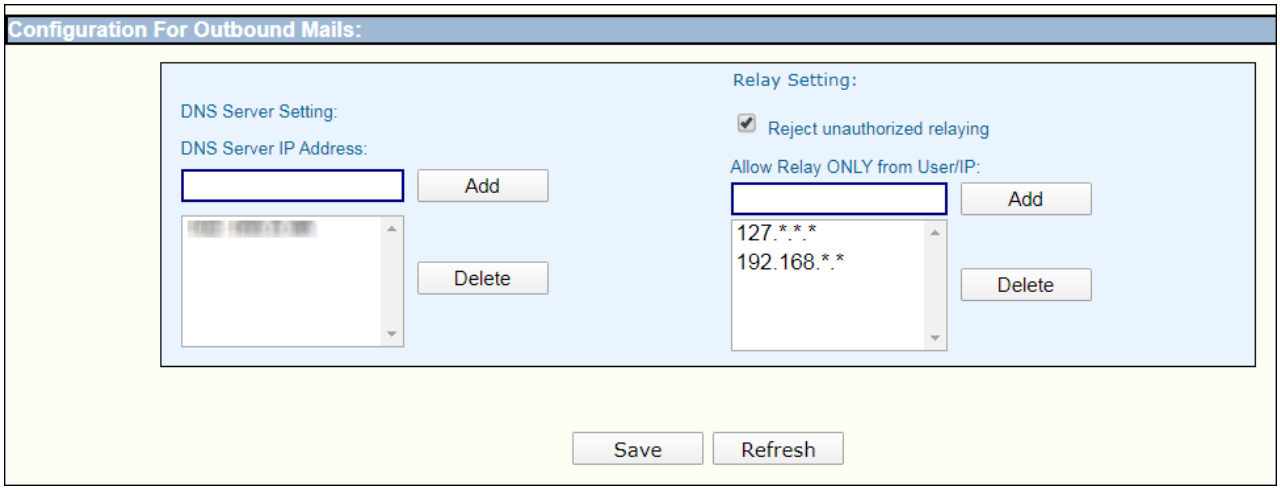


Click **OK**. This will restart the SMTP Service.

Note	If you click **Cancel**, the changes will be saved but it may not be completely effective till service is restarted.

Configuration For Outbound Mails

This section lets you configure the settings for outbound emails.



DNS Server Setting

Whenever you send an email, the SMTP server connects to a DNS server and tries to find the IP address of a recipient's domain. This section lets you add the DNS servers' IP addresses that MailScan should use while querying for information about the recipient's domain.

- **DNS Server IP Address/Add:** To add an IP address, enter the DNS server's IP address and click **Add**.
- **Delete:** To delete an IP address, select an IP address from the list and click **Delete**.

Relay Setting

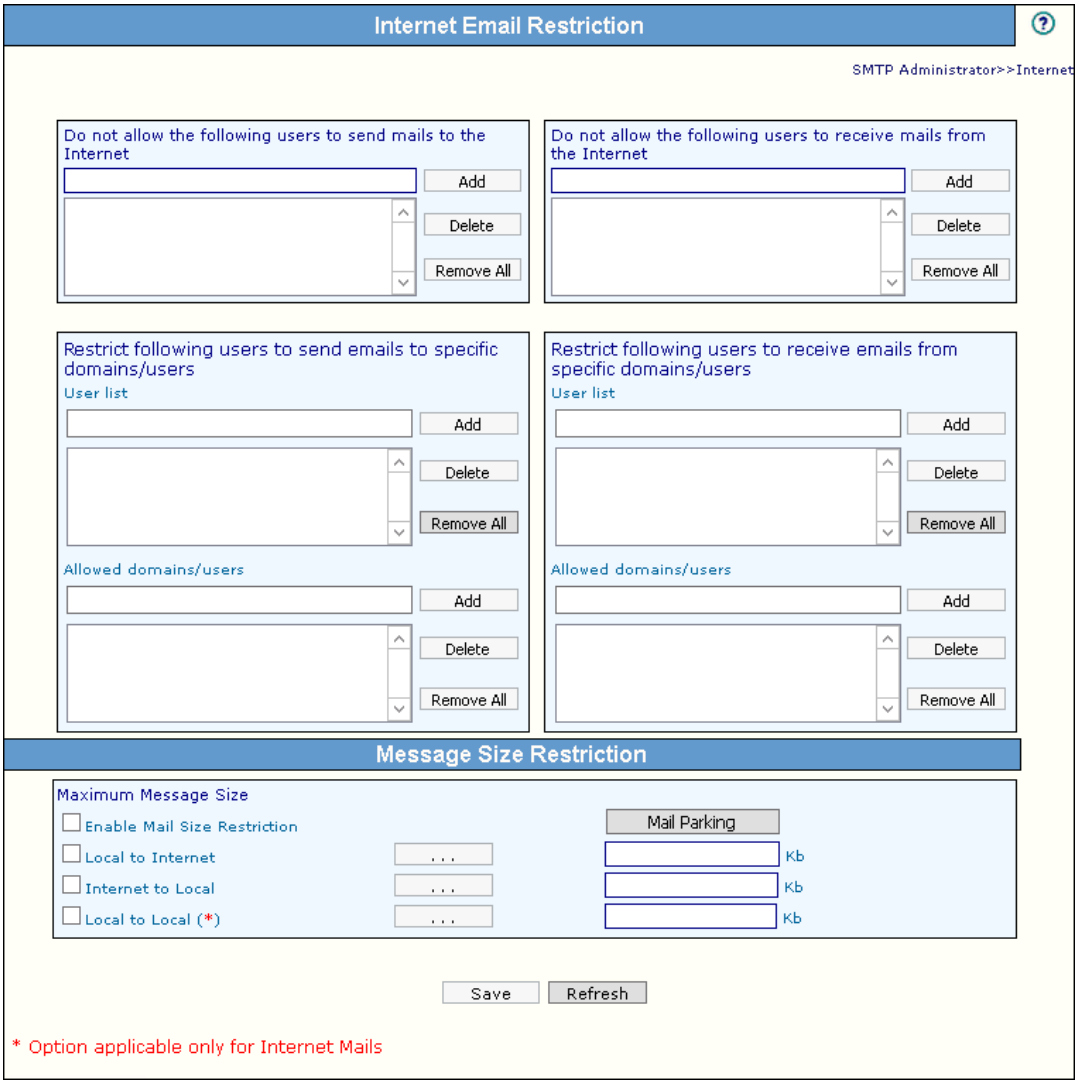
When a mail server, program or device has to redirect an email to another destination, the process is called Mail Relay. The Relay Setting section lets you configure the settings for relaying emails.

- **Reject unauthorized relaying**: Select this option if you want to prevent the mail server from relaying emails from users or IP addresses that are not present in the relay list. This helps you control spam.
- **Allow Relay ONLY from User/IP:** Specify the IP address or user name from which you want to permit the relaying of emails.
    - **Add:** Click this button to add the user name or IP address to the relay list.
    - **Delete:** Click this button to remove the user name or IP address from the relay list.

User and Mail Restriction

Internet

This submodule lets you configure User restriction settings for sending and receiving emails from and to through internet.



Do not allow the following users to send mails to the Internet

This option lets you restrict users from sending emails. You can create a list of users that will be restricted from sending emails to the internet/foreign domains.

- **Add**: Enter the email address of the user and click **Add**.
- **Delete**: Select the email address and click **Delete**.
- **Remove All**: This will remove all the email addresses from the list.

Do not allow the following users to receive mails from the Internet

This option lets you restrict users from receiving emails. You can create a list of users that will be restricted from receiving emails from internet/foreign domains.

- **Add**: Enter the email address of the user and click **Add**.
- **Delete**: Select the email address and click **Delete**.
- **Remove All**: This will remove all the email addresses from the list.

Restrict following users to send emails to specific domains/users

This option lets you to restrict the user to send emails to specific domains or users. You can create restricted list of users along with respective list of domains or users for sending emails.

- **Add**: Enter the email address of the user and click **Add**.
- **Delete**: Select the email address and click **Delete**.
- **Remove All**: This will remove all the email addresses from the list.

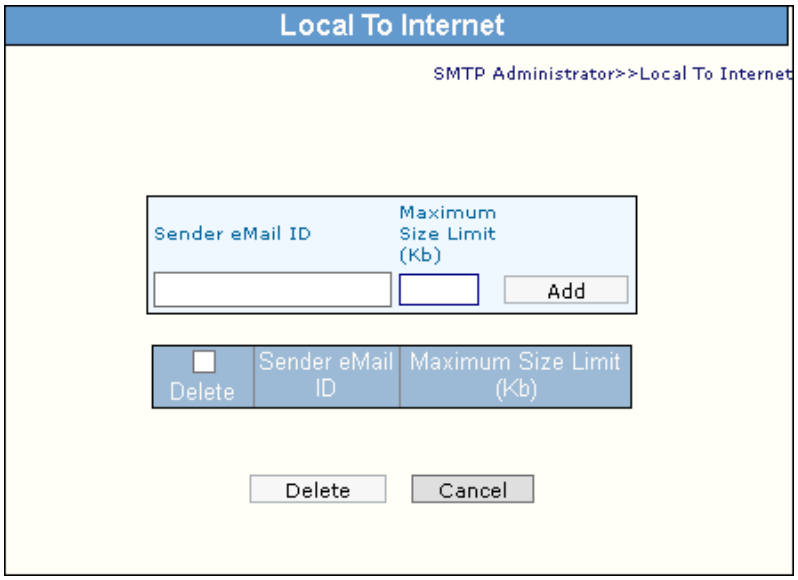
Restrict following users to send emails to specific domains/users

This option lets you to restrict the user to receive emails from specific domains or users. You can create restricted list of users along with respective list of domains or users for receiving emails.

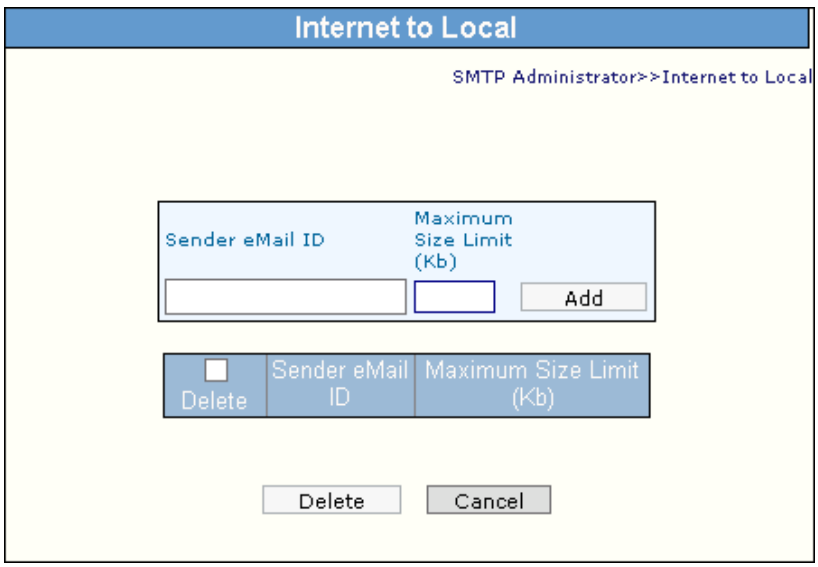
- **Add**: Enter the email address of the user and click **Add**.
- **Delete**: Select the email address and click **Delete**.
- **Remove All**: This will remove all the email addresses from the list.

Message Size Restriction

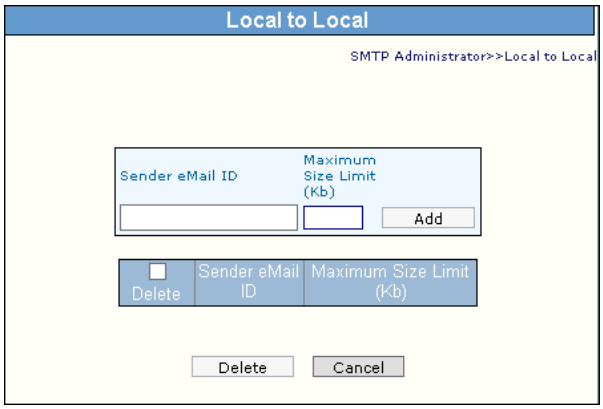
- **Enable Mail Size Restriction**: Selecting this checkbox lets you restrict size of incoming and outgoing mails.
- **Local to Internet:** Select the checkbox to restrict size of emails sent from your local domain to the Internet. Click the ellipsis button to add email ID of the sender and define size limit for the email ID.



- **Internet to Local**: Select the check box to restrict size of emails sent from the Internet to your local domain. Click the ellipsis button to add email IDs and define the maximum size limit. This will restrict mail size for specified users.

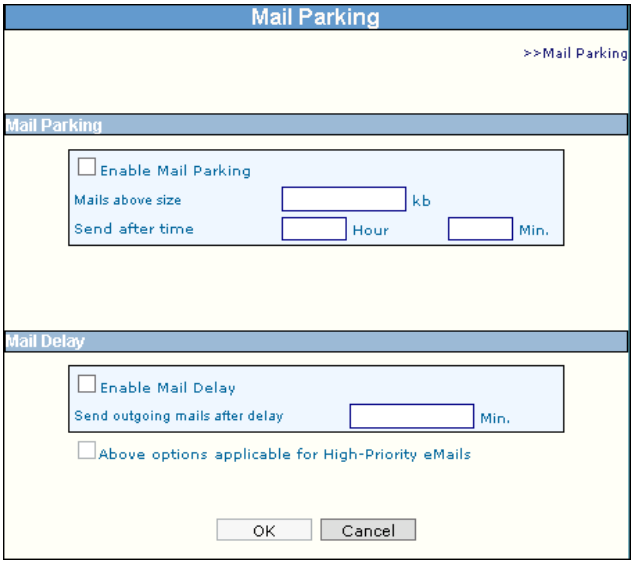


- **Local to Local**: Select the check box to restrict size of mails sent from local to local domain. Click the ellipsis to add email IDs and define the maximum size limit. This will restrict mail size to/from specified users.



Mail Parking

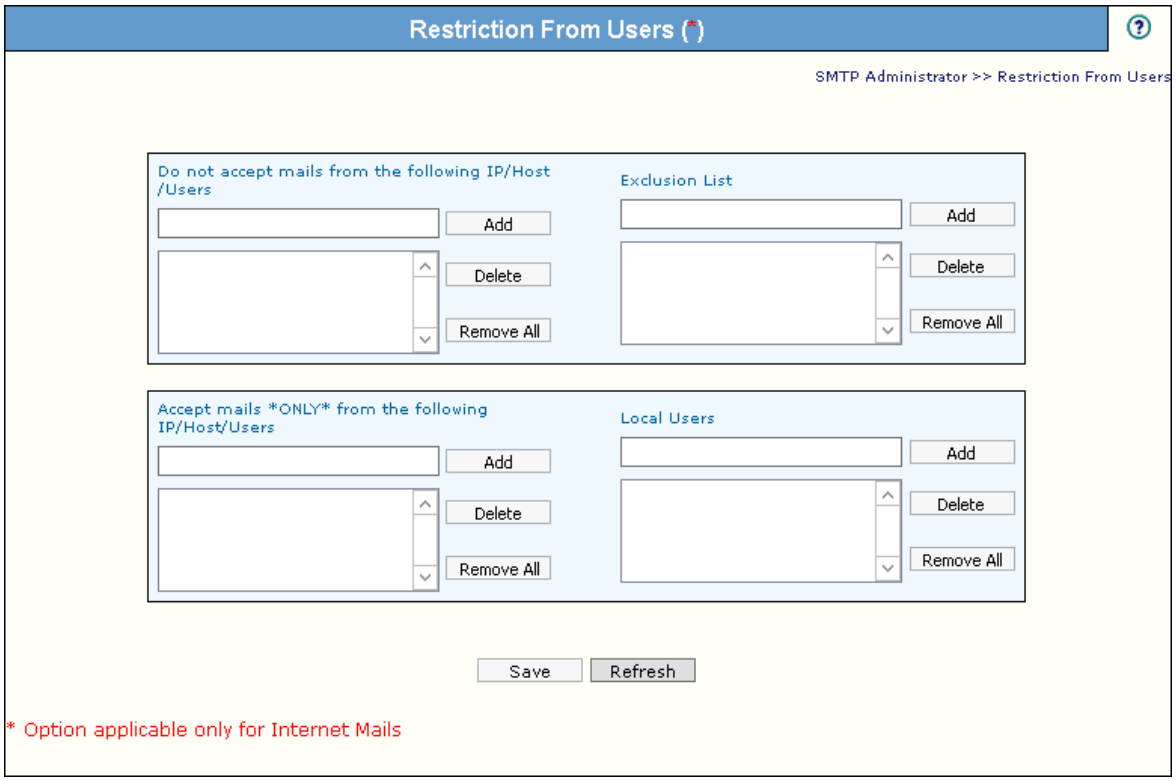
Clicking **Mail Parking** lets you configure Mail Parking and Mail Delay features. You can configure the email size, whether it should be parked or delayed, and set the time duration for this action.



- **Mail Parking**: To enable Mail Parking feature, select the checkbox **Enable Mail Parking**. You can also configure the size in KBs beyond which the emails will be parked, also define the time in hours and minutes (24 - Hour format) in respective textboxes after which the parked emails will be sent.
- **Mail Delay**: The feature lets you set the time after which the email will be allowed to pass through the gateway. To enable Mail Delay feature, select the checkbox **Enable Mail Delay** and enter the time period in minutes after which the email should be allowed to pass through the gateway.
- **Above options applicable for High-Priority eMails**: Enable this checkbox to set the above configurations for the high-priority emails.

Restriction From Users

This submodule lets you apply restrictions for receiving mails from users.



Do not accept mails from the following IP/Host/Users

This section lets you create a list of IP addresses, Host names, or email addresses from where the emails should not be accepted.

- **Add**: Enter the email address/IP address/Host name and click **Add**.
- **Delete**: Select an entry from the list and click **Delete**.
- **Remove All**: To clear the list of all entries, click **Remove All**.

Exclusion List

This section lets you create an exclusion list of IP addresses, Host names, or email addresses from where the emails will be accepted even if they are in the **Do not accept emails from the following IP/Host/Users** list.

- **Add**: Enter the email address/IP address/Host name and click **Add**.
- **Delete**: Select an entry from the list and click **Delete**.
- **Remove All**: To clear the list of all entries, click **Remove All**.

Accept mails *ONLY* from the following IP/Host/Users

This section lets you create a list of IP addresses, Host names, or user email addresses only from where the emails should be accepted. It also lets you create a list of local users only to which the received mails will be delivered.

- **Add**: Enter the email address/IP address/Host name and click **Add**.
- **Delete**: Select an entry from the list and click **Delete**.
- **Remove All**: To clear the list of all entries, click **Remove All**.

Local Users

This section lets you create a list of local users whose emails can be accepted.

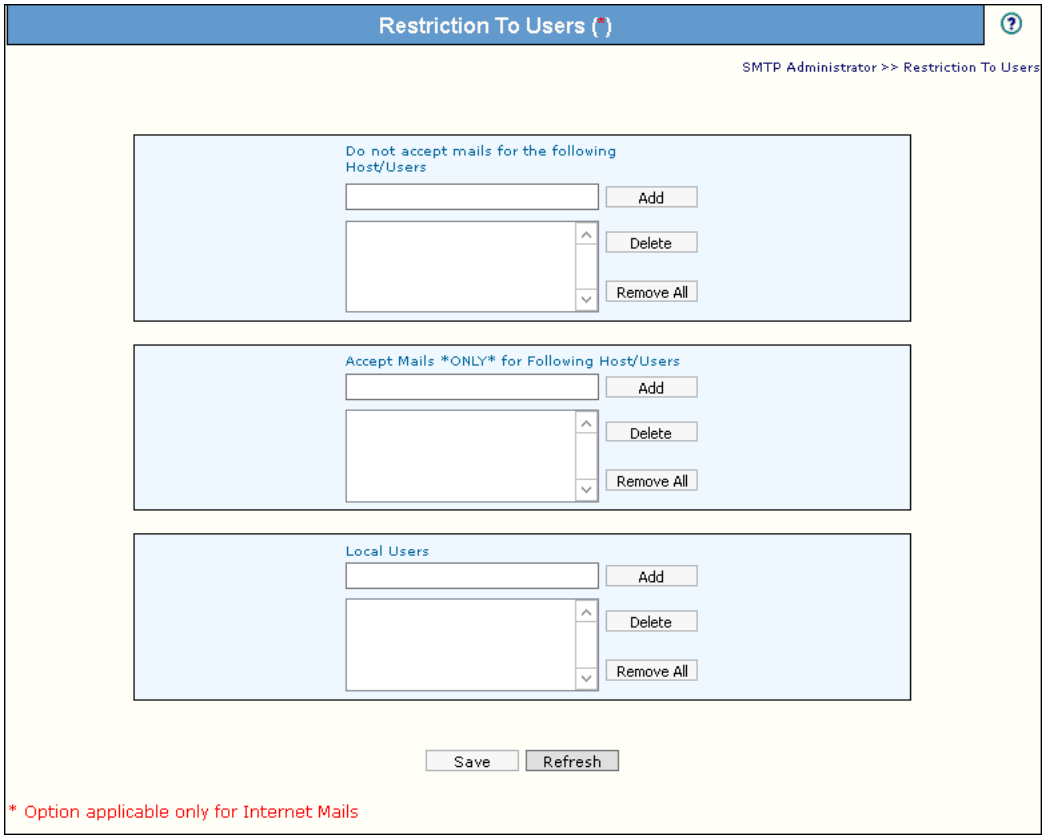
- **Add**: Enter the email address of the local user and click **Add**.
- **Delete**: Select the user from the list and click **Delete**.
- **Remove All**: To clear list of local users, click **Remove All**.

Click **Save** to save the configured setting and **Refresh** to refresh the interface.

Note	By default, the local uses list is empty which means, all users are treated as valid. If any entry is added here, only those users are treated as local and emails will be accepted from/for those users only.

Restriction To Users

This submodule lets you apply restriction to users from receiving mails.



Do not accept mails for the following Host/Users

This section lets you define Hosts/email IDs for which the emails should not be accepted. (It means the emails addressed to these users will be filtered out).

- **Add**: Enter the email/IP address of the Host/ User and click **Add**.
- **Delete**: Select a Host/User from the list and click **Delete**.
- **Remove All**: To clear list of Host/User, click **Remove All**.

Accept Mails *ONLY* for Following Host/Users

This section lets you define the Hosts/Users for which the emails should be accepted. The emails sent to these users will be allowed.

- **Add**: Enter the email/IP address of the Host/User and click **Add**.
- **Delete**: Select a Host/User from the list and click **Delete**.
- **Remove All**: To clear list of Host/User, click **Remove All**.

Local Users

This section lets you create a list of local users whose mails can be accepted.

- **Add**: Enter the email/IP address of the Host/User and click **Add**.
- **Delete**: Select a Host/User from the list and click **Delete**.
- **Remove All**: To clear list of Host/User, click **Remove All**.

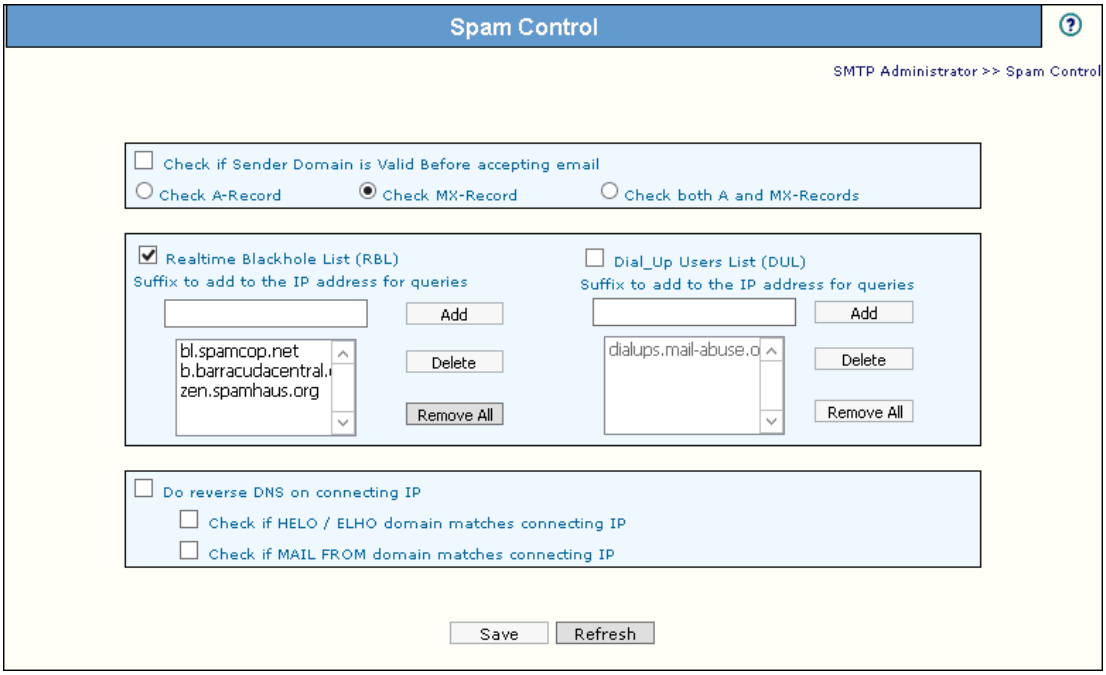
Note	By default, the local uses list is empty which means, all users are treated as valid. If any entry is added here, only those users are treated as local and emails will be accepted from/for those users only.

Spam Control

This submodule lets you configure settings and greylist the IP addresses.

Settings

This submodule lets you configure settings to control spam. It lets you verify whether the email sender's domain is valid before accepting emails.



Check if Sender Domain is valid before accepting email

Selecting this checkbox enables MailScan to verify if the sender domain is valid before accepting an email. You can ensure that the following items are checked:

- **Check A-Record**: A Record stands for Address Record. Record determines which IP address belongs to a domain name. This record translates the domain name to an IP address. Selecting this option enables MailScan to check A Record.
- **Check MX-Record**: MX Record stands for Mail Exchange Record. It is a type of resource code in DNS. This record indicates to what specific IP address emails needs to be sent. Selecting this option enables MailScan to check MX Record.
- **Check both A and MX-Records**: Selecting this option enables MailScan to check both A and MX Records.

Real-time Blackhole List (RBL)

Organizations like MAPS (Mail Abuse Prevention System) provide a list of IP addresses that are known Spammers. This list is called Real-time 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 this checkbox to check with the RBL and verify if the sender domain is valid, before accepting email.

- **Add**: Enter the Domain name and click **Add**.
- **Delete**: Select a Domain name from the list and click **Delete**.
- **Remove All**: To clear list of domains, click **Remove All**.

Dynamic/Dial-up Users List (DUL)

Few 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 which carry details of known Spammers is displayed. Enter the suffix to add to the IP address for queries and click Add. Refer DUL.

- **Add**: Enter the Domain name and click **Add**.
- **Delete**: Select a Domain name from the list and click **Delete**.
- **Remove All**: To clear list of domains, click **Remove All**.

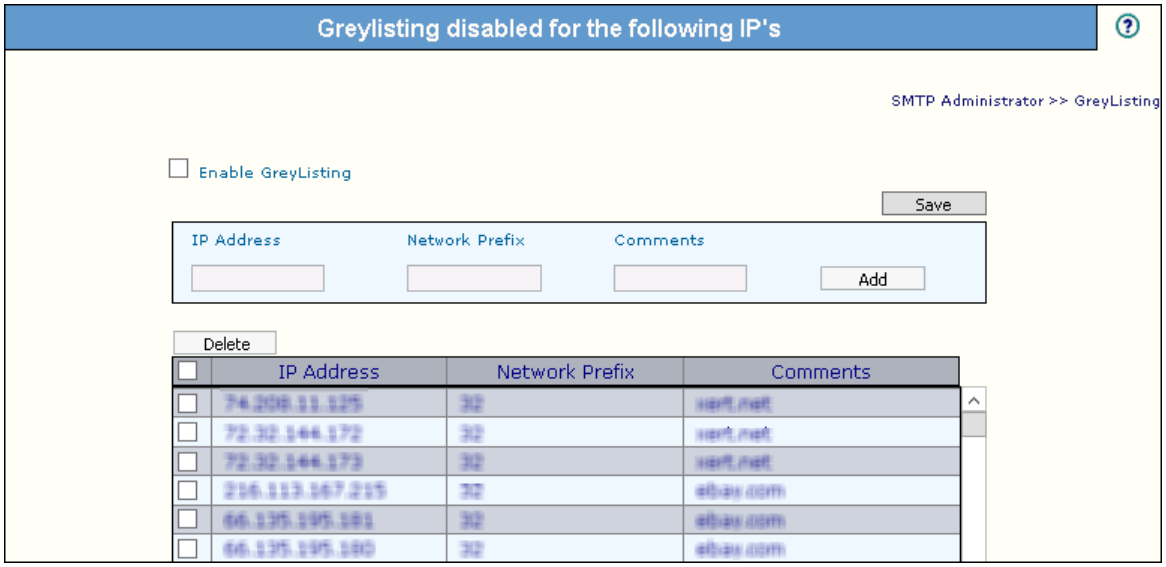
Do reverse DNS on connecting IP

When other users try to connect to your server, you can run a reverse DNS to verify their IP address.

- **Check if HELO/ELHO domain matches connecting IP**: This is a request made to the SMTP server by a client. This allows two SMTP servers 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.
- **Check if Mail FROM domain matches connecting IP**: Spammers send emails through another (spoofed) IP. After selection, MailScan verifies the IP of the email ID in the From box is the same as the connecting IP.

GreyListing

Greylisting is a method of blocking spam by temporarily rejecting emails coming from unknown senders. If the email is legitimate, the originating server in most cases will re-attempt to send it, which will then be accepted by the recipient mail server. It is observed that most spamming servers do not try to resend the email in case of a first time rejection.



The Greylisting submodule records following information from each incoming email:

- IP address of the Host
- Sender email ID
- Recipient email ID

Greylisting an IP address

To Greylist an IP address, follow the steps given below:

1. Select the checkbox **Enable Greylisting**.
2. In the IP address box, enter the IP address.
3. In the Network Prefix box, enter number of bits. The value must be less than or equal to 32. If null value or zero is entered, then value will be considered as 32 bits.
4. In the Comments box, enter a reason/description for Greylisting.
5. Click **Add.** The IP address gets Greylisted.

Deleting a Greylisted IP address

To delete a Greylisted IP address, select an IP address from the list and click **Delete**. The Greylisted IP address gets deleted.

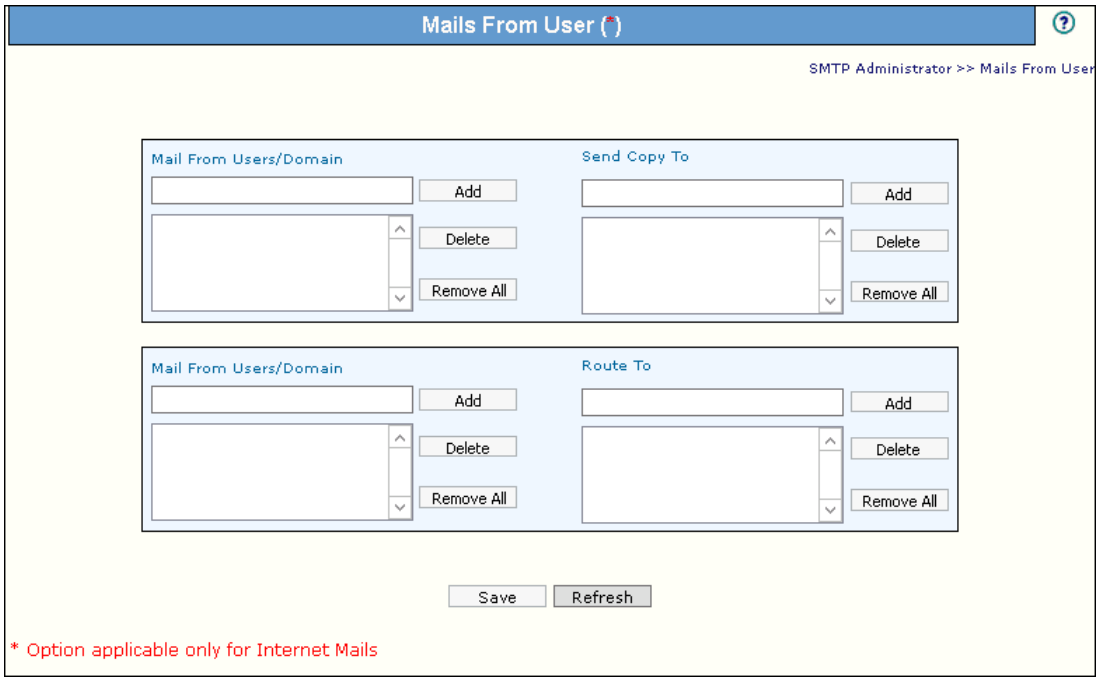
Click **Save** to save the configure setting.

User Based Rulesets

This submodule lets you define rules for users/domains.

Mails From User

You can configure MailScan to send a copy to or route any email sent from the user/domain listed to email IDs or domain specified by you.



Mail From Users/Domain

Enter the email ID/domain in this box and then click **Add**. A copy of emails sent by user/domain will be sent to user or domain as specified by you in **Send Copy To** box.

Send Copy To

Enter an email ID in this box and then click **Add**. Copy of emails received from specific email IDs/domains specified by you in **Mail From Users/ Domain** will be sent to the email ID in the list.

Mail From Users/Domain

Enter the email ID/domain in this box and then click Add. Emails sent by users/domain will be routed to email ID selected in the **Route To** box.

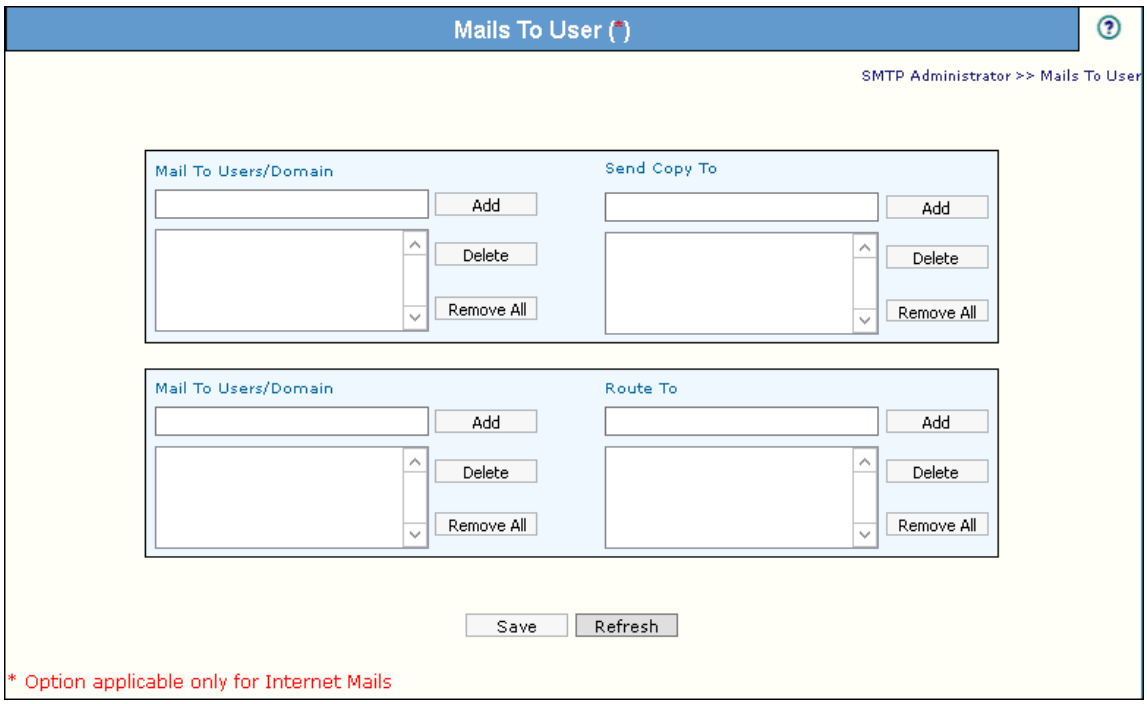
Route To

Enter an email ID in this box and then click **Add**. Emails sent by users/domain listed in the **Mails From Users/Domains** will be routed to the email ID selected in the list.

Click **Save** to save the configured settings and **Refresh** to refresh the UI.

- **Add**: Enter the domain/email address and click **Add**.
- **Delete**: Select a domain/email address from the list and click **Delete**.
- **Remove All**: To clear list of all the entries, click **Remove All**.

Mails To User



Mail To Users/Domain

Enter the email ID/domain in this box and then click **Add**. A copy of emails sent by user/domain will be sent to user or domain as specified by you in **Send Copy To** box.

Send Copy To

Enter an email ID in this box and then click **Add**. Copy of emails received from specific email IDs/domains specified by you in **Mail To Users/ Domain** will be sent to the email ID in the list.

Mail To Users/Domain

Enter the email ID/domain in this box and then click Add. Emails sent by users/domain will be routed to email ID selected in the **Route To** box.

Route To

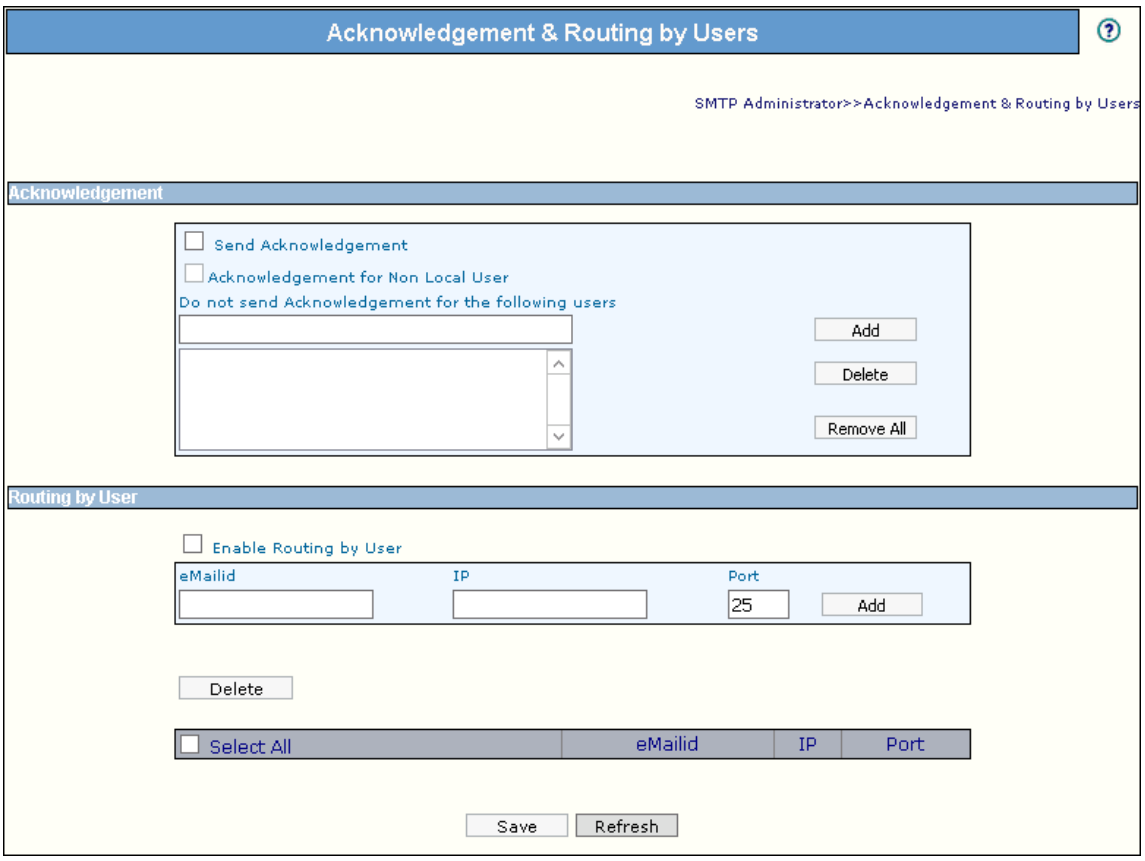
Enter an email ID in this box and then click **Add**. Emails sent by users/domain listed in the **Mails To Users/Domains** will be routed to the email ID selected in the list.

Click **Save** to save the configured settings and **Refresh** to refresh the UI.

- **Add**: Enter the domain/email address and click **Add**.
- **Delete**: Select a domain/email address from the list and click **Delete**.
- **Remove All**: To clear list of all the entries, click **Remove All**.

Acknowledgement & Routing by Users

This module has two configurations, namely, **Acknowledgement** and **Route by**.



Acknowledgement

An acknowledgement is an indication that the message has reliably arrived at its destination. This section lets you configure sending an acknowledgement for local and non-local users. You can also configure to stop sending acknowledgements to selected users. You can add, delete, or remove all the users from the list as per your convenience.

- **Send Acknowledgement**: Select this checkbox to send an acknowledgement to a user within your network.
- **Acknowledgement for non-local user**: Select this checkbox to send an acknowledgement to a user outside your network.
- **Do not send Acknowledgement for the following users**: You can create a list of users to whom you don't want to send an acknowledgement.

- **Add**: Enter the email address of the user and click **Add**. The acknowledgement will not be sent to the user.
- **Delete**: Select an email address from the list and click **Delete**.
- **Remove All**: To clear list of all the entries, click **Remove All**.

Routing by User

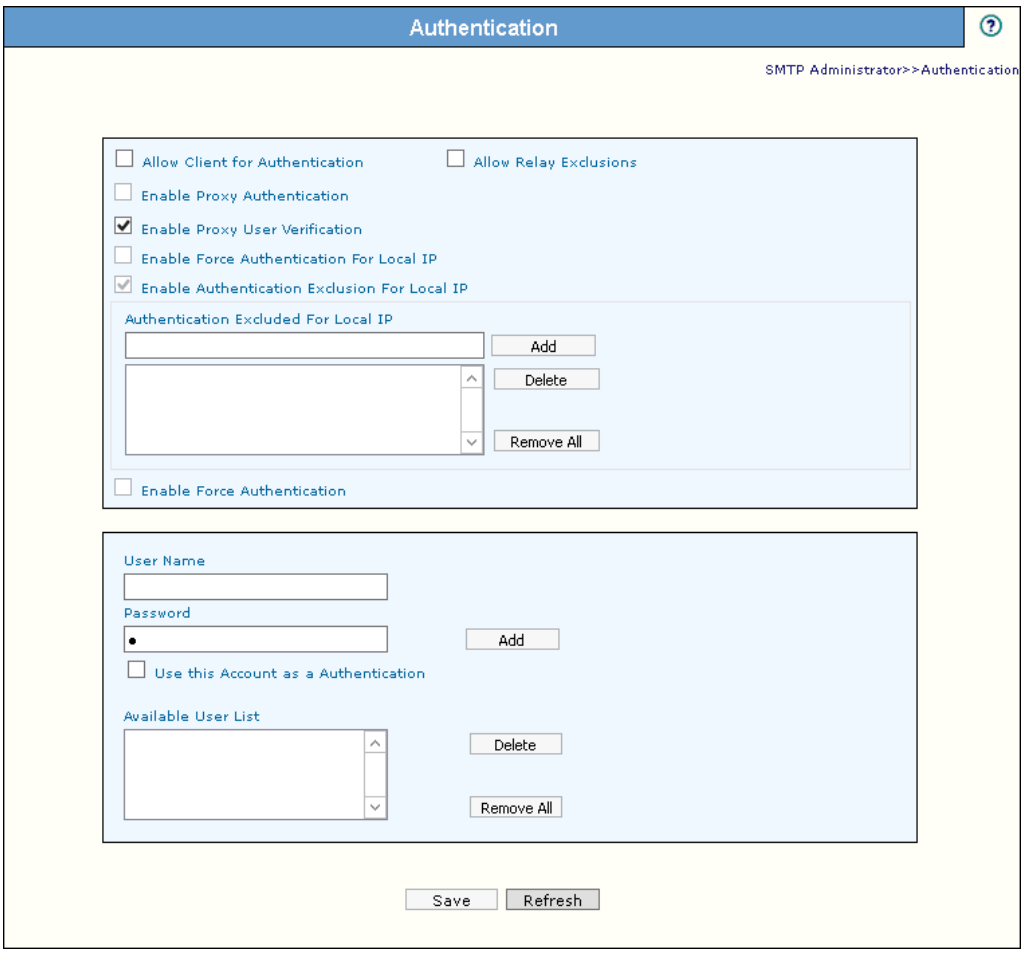
This section lets you configure MailScan to route emails addressed to specific users to another email server.

To enable routing by user, follow the steps given below:

1. Select the checkbox, **Enable Routing by User**.
2. In the **eMailid** textbox enter the specific user's email ID.
3. In the **IP** textbox, enter the IP address of the routing email server.
4. In the **Port** textbox, enter the port number.
1. Click **Add**. The user gets added to Routing by User list.
5. Click **Save**.

Authentication

This submodule lets you configure the authentication settings for incoming and outgoing emails.



- **Allow Client for Authentication**: Select this checkbox to authenticate the client for the incoming and outgoing emails. Selecting this checkbox lets you select **Enable Force Authentication**, **Enable Proxy Authentication**, and **Enable Force Authentication For Local IP** options.
- **Enable Proxy Authentication**: Select this checkbox to authenticate the proxy used by clients for the incoming emails.
- **Enable Proxy User Verification**: Select this checkbox to verify the proxy users. Every time the proxy is used it will be verified. If the verification fails, all incoming and outgoing emails will be blocked.
- **Enable Force Authentication for Local IP**: Select this checkbox to force run authentication process only on the local IP address. If the authentication fails, the incoming emails will be blocked.
- **Enable Authentication Exclusion for Local IP**: Select this checkbox to exclude the local IPs from the authentication process. After selection, all incoming and outgoing mails between the local IP shall be allowed.

- **Authentication Excluded for Local IP**: Local IP address added to this list will be excluded from authentication.
  Enter the Local IP address and click **Add**. You can delete the IP address that does not require any further authentication. It will also allow you to remove all the IP addresses that require authentication.
- **Enable Force Authentication**: Select this checkbox to force authentication process on all the incoming mails.
- **Allow Relay Exclusions**: Select this checkbox to allow the relay exclusions (outbound emails) for the authenticated IP addresses.

Adding User for authentication

To add user, perform following steps:

1. Enter **User Name** and **Password** for creating account.
2. If you want use this account for authentication, select **Use this Account as a Authentication** checkbox.
3. Click **Add**. The user will be available in the **Available User List**.

Deleting the User

To delete the user from the list, select the user and click **Delete**.

Remove All

To clear all the user from the list, click **Remove All**.

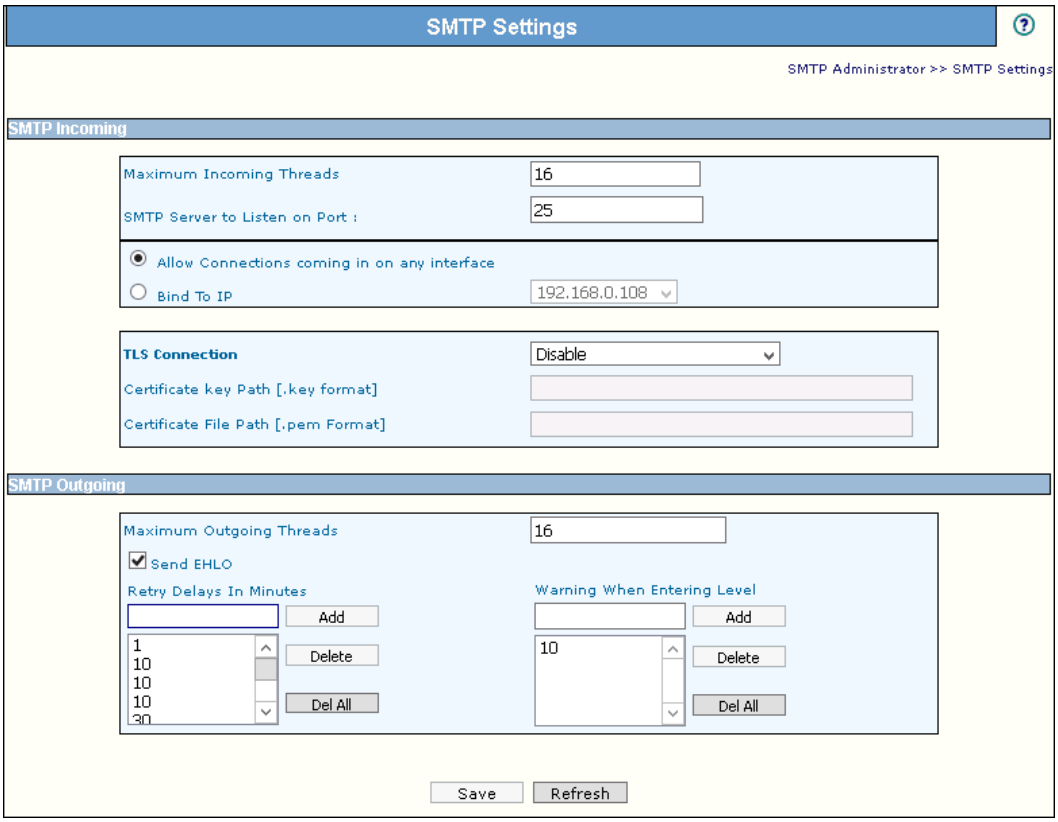
Click **Save**, to save the configured setting and **Refresh** to refresh the UI.

Server Settings

This module lets you to configure the SMTP settings, controls, proxy, and more.

SMTP Settings

This option lets you configure the SMTP server settings for the incoming and outgoing emails that hit the MailScan SMTP server.



SMTP Incoming

This section lets you configure settings for the incoming emails that hit the SMTP server. You can also define the settings as in whether to allow the connection to free flow in to any interface or bind it to any particular IP address.

- **Maximum Incoming Threads**: Define the maximum incoming thread count for simultaneous incoming connections with remote SMTP server. It depends on the configuration of the system where mail server is hosted. Default thread count is 16.
- **SMTP Server to Listen on Port**: Define the port number where SMTP server will listen for incoming emails.
- **Allow Connections coming in on any interface**: Select this option to allow the incoming email connection free flow into any interface.
- **Bind To IP**: Select this option to bind the incoming email connection to a particular IP address. Selecting this option enables the IP address dropdown. Click the dropdown and select the specific IP address.

- **TLS Connection**: This option allows you to Enable and add Certificate file and Certificate key to facilitate encrypted communication through mail server.
    - **Certificate key Path [.key format]**: If **TLS Connection** is enabled; you have to provide the path for the certificate KEY.
    - **Certificate File Path [.pem Format]**: If **TLS Connection** is enabled; you have to provide the path for the certificate file in PEM format.

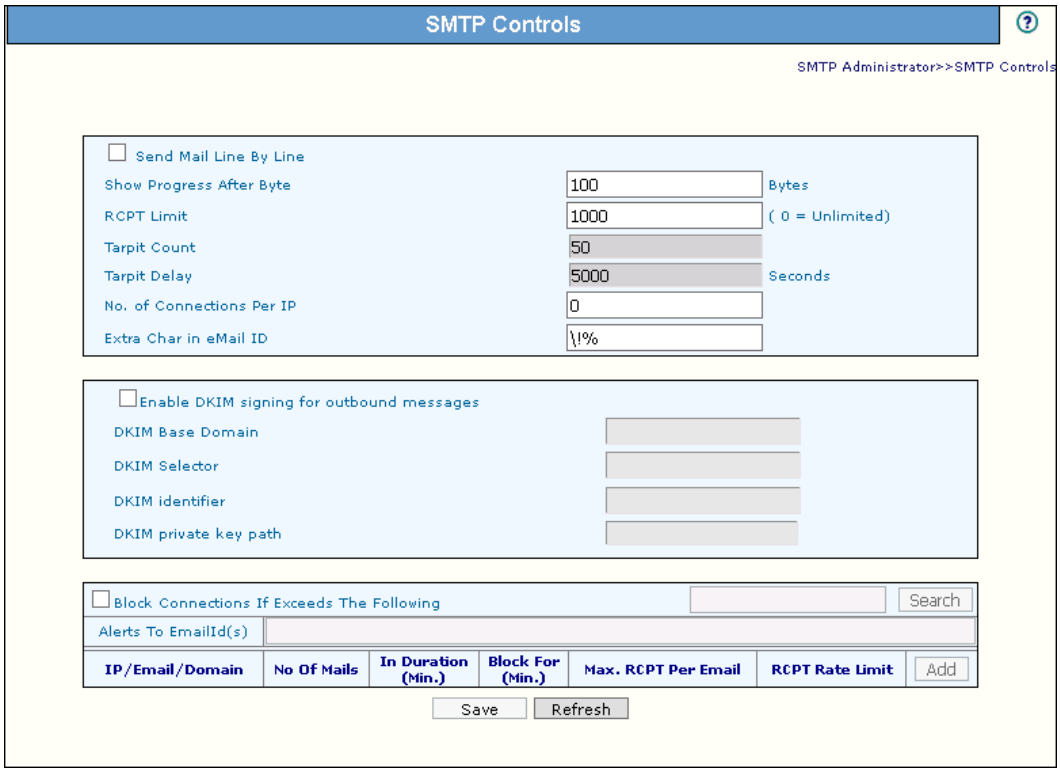
SMTP Outgoing

This section lets you configure the settings for the outgoing emails that leave the MailScan server. You can also configure the settings for retrying delay time as well as the warning on entry level.

- **Maximum Outgoing Threads**: Define the maximum outgoing thread count for simultaneous outgoing connections with remote SMTP server. It depends on the configuration of the system where Mail Server is hosted. Default thread count is 16.
- **Send EHLO**: Select this option to send EHLO command to the receiving server to initiate the connection.
- **Retry Delay in Minutes**: Specify the time to retry sending EHLO command after the first delay. The first retry will happen in one minute or whatever limit you specify. MailScan reattempts sending the email after the specified time interval.
- **Warning when Entering Level**: Define the time limit to send a warning, when EHLO command fails to get a response. The warning will be sent to the original sender that there is no response on the EHLO message sent.

SMTP Controls

This submodule lets to configure SMTP control settings for the emails that pass through Mail Server.

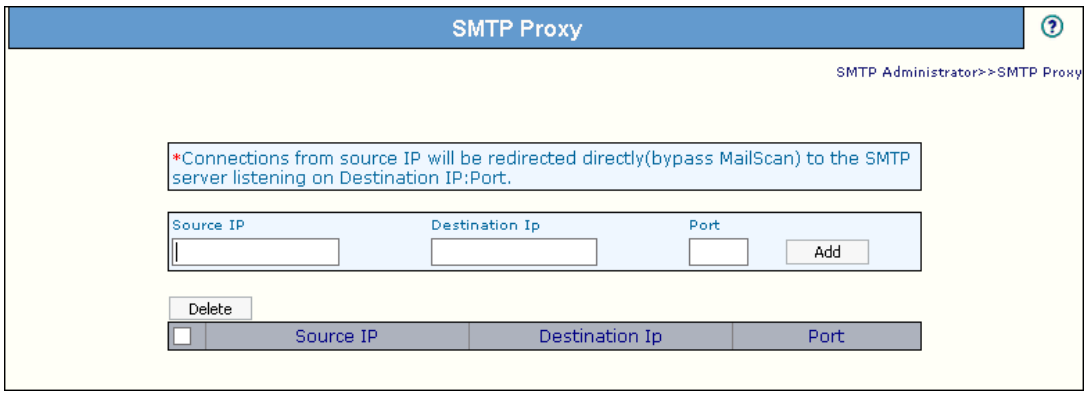


- **Send Mail Line by Line**: Select this checkbox to send an email line by line. After selecting, you will be notified about the progress of the sent email based on the attachment size. This option ensures that the clarity is retained in forwarded emails but in this process, the time taken to send an email will be more.
- **Show Progress After Byte**: Define the size of byte to display the progress of the incoming/outgoing email. You will be able to see the progress of the email after the specified bytes of the attachment is transferred.
- **RCPT Limit**: Enter the total RCPT limit (recipients in the CC field) for the mails sent through your mail server. If you want your email to be received by unlimited recipients at a time then set the limit as '0'.
- **Tarpit Count**: Tarpit is a service that purposely delays incoming connections to avoid email spamming. Tarpit count will specify the number of recipients after which the delay will be inserted in between the SMTP session of each RCPT TO.
- **Tarpit Delay**: Define the time interval (in seconds) of delay to introduce after each subsequent RCPT TO.
- **No. of connections Per IP**: Define the number of connections allowed for a particular IP address. '0' specifies unlimited connections or set it to a minimum number of connections. This will help you in tracking down the IP address that are broadcasting on the SMTP port in case of infection and lot of spam and malicious emails being sent using the SMTP server.

- **Extra Char in email ID**: Enter the extra characters that cannot be used in the email ID. Emails that have any of these characters in the TO address will not be downloaded by the server, but will be rejected outright. This will help you reduce spam count.
- **Enable DKIM signing for outbound messages**: Select this checkbox to enable the DKIM signing to emails. DKIM is a form of email authentication that allows an organization to claim responsibility for a message in a way that recipients can validate.
- **DKIM Base Domain**: Enter the signing domain name identifier.
- **DKIM Selector**: Enter the selector to validate the DKIM signing. A selector is added to the domain name, used to find DKIM public key information.
- **DKIM identifier**: Enter a string that may identify the site to you when you look at the Authentication-Results message header. Use the syntax of a fully qualified domain name
- **DKIM private key path**: Private key (If not available) is to be generated using open source tools and stored in .pem format. Mention that key path here.
- **Block Connections if exceeds the following**: Select this checkbox to configure the **SMTP Rate Limit** options. In **SMTP RATE LIMIT**, if the mail flow from particular user of given domain OR email id OR IP address exceeds the set limit within given time period (as configured), the sender email id will be blocked for specific time. You will get the following options:
    - **Alert to email ID(s)**: If the SMTP Rate limit threshold is reached, an alert about the incident will be sent to the emails ID(s) entered in this list.
    - **IP/email/ Domain**: Add the IP address/email/domain for which SMTP rate limit is to be implemented.
    - **No. of mails**: Specify the maximum number of mails from the specified IP/email/Domain. Sender email ID will be blocked if the count exceeds beyond the set number of mails.
    - **In duration**: Specify the time duration (in minutes) to be considered for SMTP Rate Limit. Time is calculated or maintained separately for individual sender once first email is received.
    - **Block for**: Specify the time limit (in minutes) for which the sender email id / IP has to be blocked; in case it meets all the above criteria.
    - **Max RCPT per email**: Specify the maximum recipients per email sent.
    - **RCPT Rate limit**: Specify the total number of recipients (in all of the sent emails) from the given sender email id / IP address within the specified time duration.

SMTP Proxy

This submodule lets you configure the settings for redirecting connections from the source IP address to the SMTP server listening on destination IP address and port without being filtered for malware and spam. The connection made will thus bypass MailScan.



Adding a SMTP Proxy

To add SMTP Proxy, perform following step:

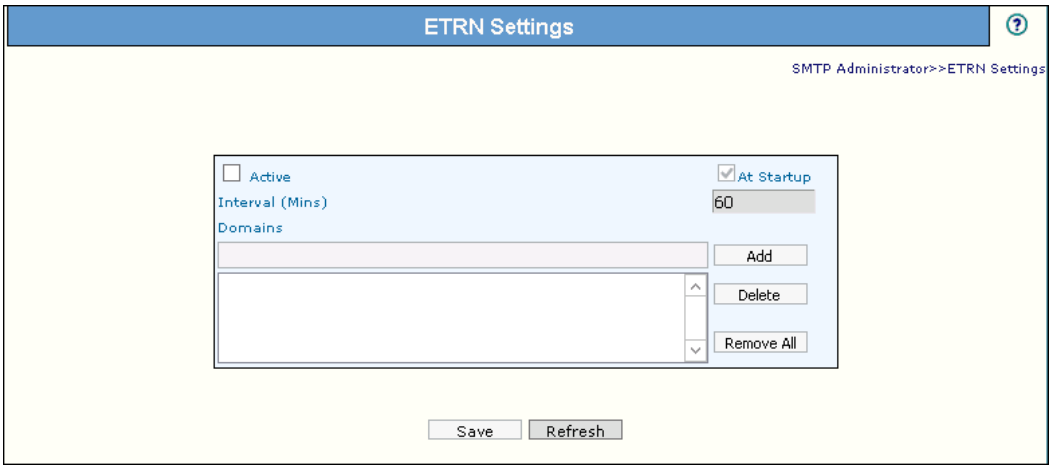
1. Enter the Source IP address, Destination IP, and Port number.
2. Click **Add**. The SMTP Proxy gets added.

Deleting a SMTP Proxy

To delete a SMTP proxy, select the proxy and click **Delete**.

ETRN Setting

This submodule lets you configure the delay in minutes of mail relay for a specific domain.

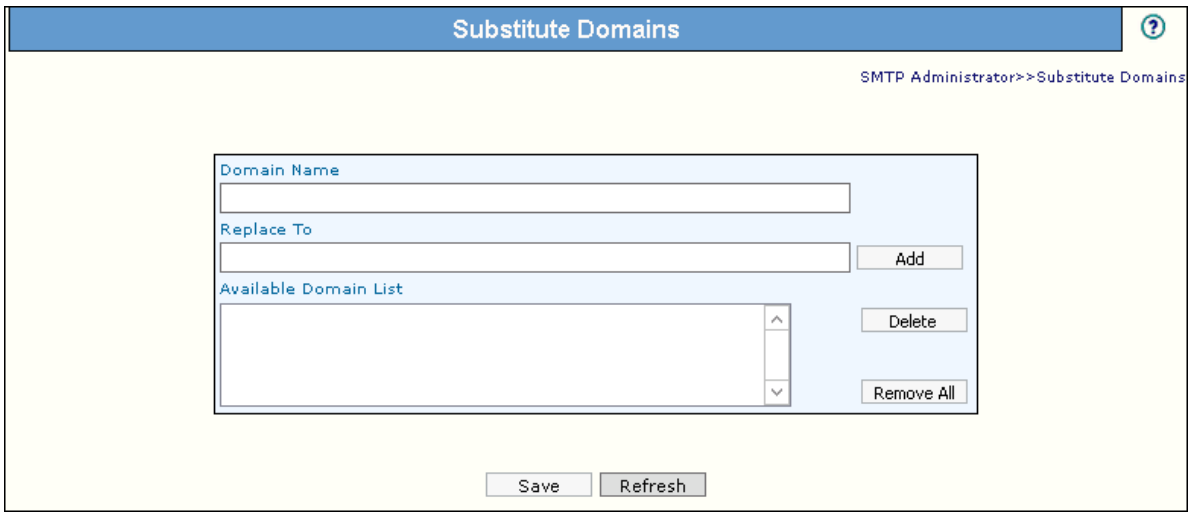


- **Active**: Select this check box to activate the delay in mail relay for a specific domain.
- **At Startup**: Selecting this check box activates ETRN feature as MailScan start up.
- **Interval (Mins)**: Specify the delay in minutes for the mail relay for the domain names specified in the list.
- **Domains**: This will allow you to add the domain names for which the delay in mail relay should be allowed.
    - **Add**: Enter the domain name for which the relay should be allowed and click **Add**.
    - **Delete**: To delete, select the particular domain and click **Delete**.
    - **Remove All**: To clear list of domain names, click **Remove All**.

After making changes, save settings by clicking **Save**.

Substitute Domains

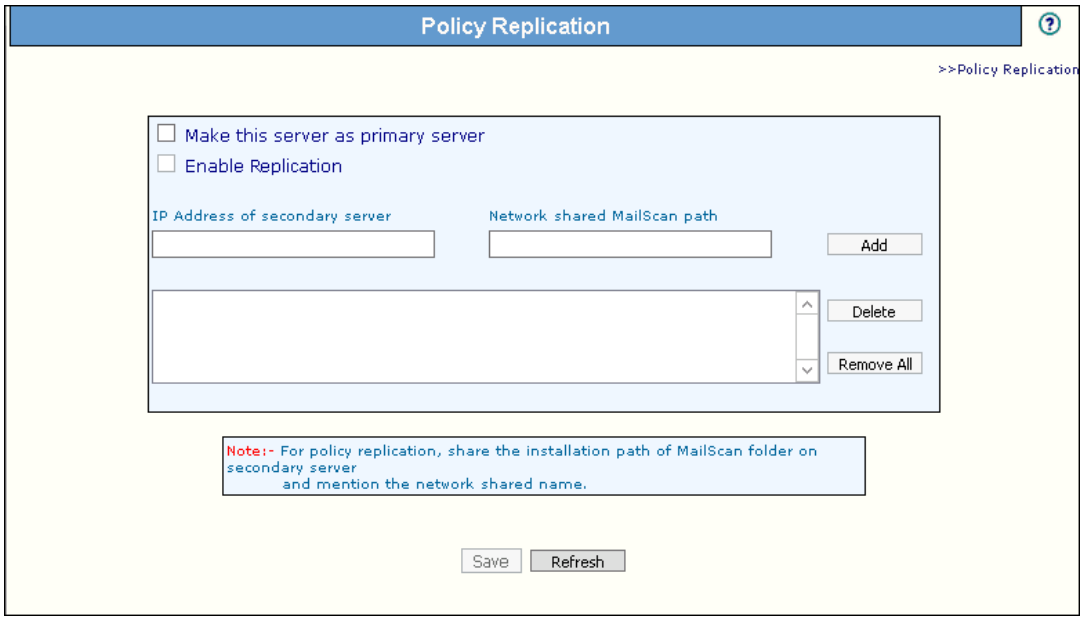
This submodule lets you configure the substitute domains in your network. It can be used to redirect mails from one domain to another or in a scenario where the current domain needs to be replaced.



- **Available Domain List**: This will display the list of source domains and replaced domain names. For example, an entry in this list might read as "abc.com, xyz.com." This means that you have replaced the source domain name "abc.com" with "xyz.com." This box lets you to substitute one domain name with another.
- **Domain Name**: In this box, enter the domain name that you wish to replace (the existing or the old domain name).
- **Replace To**: In this box, enter the domain name that you wish to replace with. The domain name specified here will replace the domain name specified in the above section.
- **Add**: After entering both the domain names, click **Add**. The domain will be added as first, second.
- **Delete**: To delete, select the domain names and click **Delete**.
- **Remove All**: To clear list of domain names, click **Remove All**.

Policy Replication

MailScan policies can be replicated across multiple servers thus reducing the administrative overhead of making policy changes across all servers manually.



- **Make this server as primary server**: Select this checkbox to make the local MailScan system as primary server.
- **Enable Replication**: Select this checkbox to enable the replication of MailScan configuration/settings to the specified secondary servers.
- **IP Address of secondary server**: Enter the IP address of the secondary server.
- **Network shared MailScan path**: Enter the installation path of MailScan folder for the secondary server.
- **Add**: After entering IP address of the secondary server and network path, click **Add**.
- **Delete**: To delete, select the IP address from the list and click **Delete**.
- **Remove All**: To clear the list, click **Remove All**.

Click **Save** to save all the configuration settings and **Refresh** to refresh the interface.

IP Whitelisting

This submodule lets you specify the IP addresses you want to exclude from spam RBL checks.

IP addresses of sites that are exempted from Spam Blocker, RBL, and Reverse DNS lookups. This list contains the IP addresses that you want to exclude from Spam Blocker, RBL checks, and Reverse DNS.

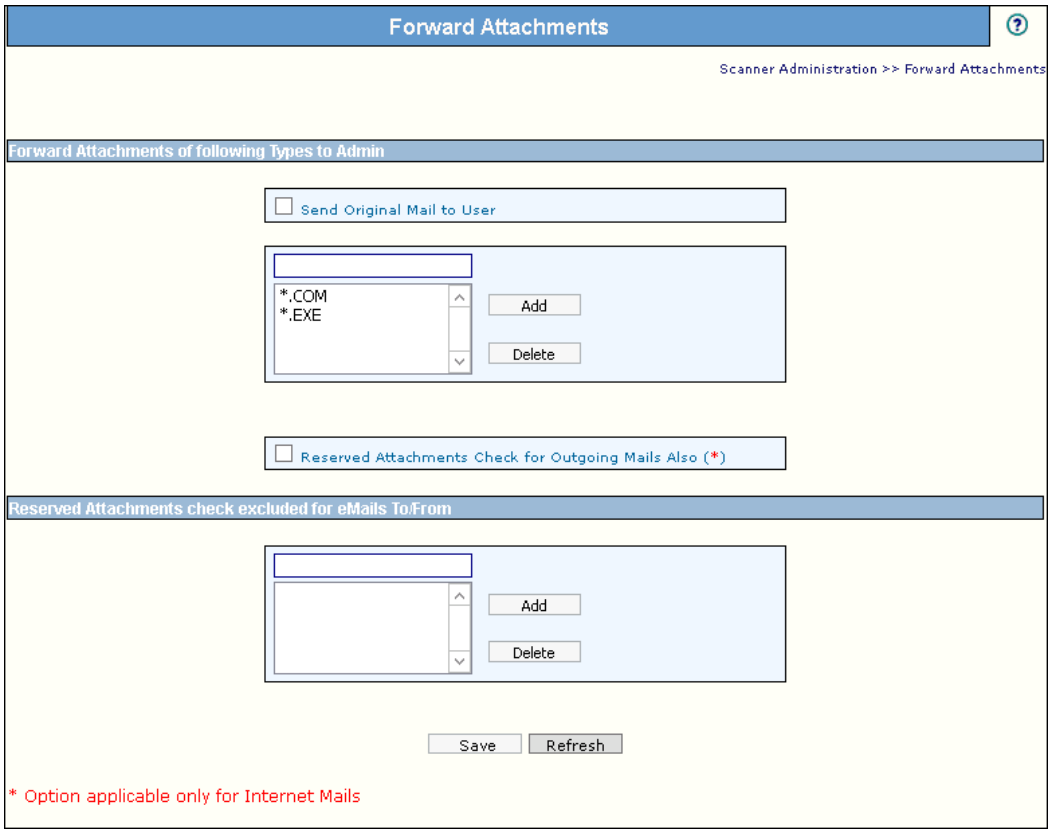
- **Add**: Enter the IP address and Click **Add**. It will be added to the list.
- **Delete**: To delete, select the IP address from the list and click **Delete**.
- **Remove All**: To clear the list of IP addresses, click **Remove All**.
- **Set to Default**: To remove the custom entries from the list and display only the default entries in the list, click **Set to Default**.

Scanner Admin

This section lets you configure the settings related to Scanner Administration. We will define the settings for Forward Attachments, Attachment Control, Action, Advanced IE Vulnerabilities and Archivals, AV Update Configuration, After Update Settings.

Forward Attachments

This page lets you configure the settings for forwarding attachments.



Forward Attachments of following Types To Admin

This section allows you to define settings to forward email attachments with specific file (usually restricted) types to the Administrator. This is especially useful to administrators because they can decide what action needs to be performed on the (suspicious) attachments. It allows you to define following settings:

- **Send Original mail to user**: Select this checkbox to send the original email to the user. This will send the email containing restricted attachments belonging to restricted file types to the recipient. Administrator will receive a copy of the email whenever MailScan detects a file containing the listed file type.

How to add File types?

- Enter a file extension by typing an asterisk, dot, and extension then click **Add**. For example, if you want to block EXE extension, enter *.EXE and click Add.
- To delete a file extension from the list, select the specific file extension and click **Delete**.

- **Reserved Attachments for Outgoing mails Also**: Select this option to check restricted attachment for outgoing emails as well.

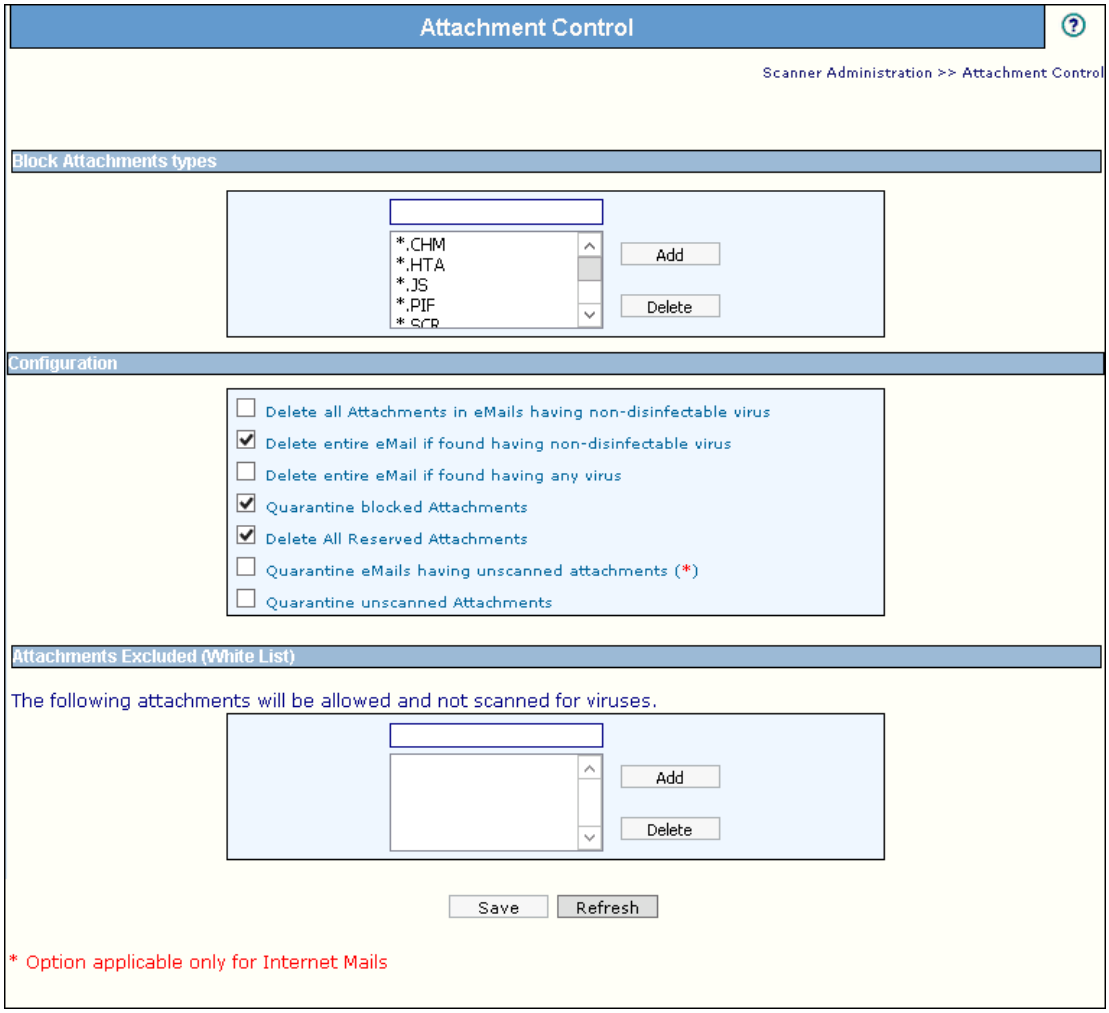
Reserved Attachments Check excluded for email To/From

This will allow MailScan to exclude the reserved attachments if received from/sent to specific email IDs. Add the specific email IDs to the list.
To add email IDs:

- Enter an email ID and click **Add**, the email IDs added to this list will be excluded from checking reserved attachments.
- To remove an email ID from the list, select the specific email ID and click **Delete**.

Attachment Control

This submodule lets you configure the settings based on attachment types.



Block Attachments types

This section will display a predefined list of file types that are often used by virus writers to embed viruses. Any email attachment having an extension included in this list will be blocked or deleted by MailScan at the gateway level. You can add file extensions for blocking as per your requirements. As a best practice, you should avoid deleting the file extensions that are present in the **Block Attachments types** list by default.

- **Add**: Enter the file extension that you want to be blocked and click **Add**. The file extension added to this list will be blocked.
- **Delete**: Click **Delete** to remove a file extension from the list to file extensions to be blocked.

Configuration

This section will allow you to configure Settings for the action to be taken on reserved and blocked file extension types.

- **Delete all Attachments in eMails having non-disinfectable virus**: Select this checkbox to delete all the attachments in email in case it cannot be cleaned.
- **Delete entire eMail if found having non-disinfectable virus**: Select this checkbox to delete entire email in case virus infection cannot be cleaned.
- **Delete entire eMail if found having any virus**: Select this checkbox to delete any email having virus.
- **Quarantine Blocked Attachments**: Select this checkbox to quarantine the email if it has the file extension that is blocked by MailScan.
- **Delete All Reserved Attachments**: Select this checkbox to delete the email if it has the file extension that is blocked by MailScan.
- **Quarantine eMails having unscanned attachments**: Select this checkbox to Quarantine all emails that have not been scanned for malware infection.
- **Quarantine unscanned Attachments**: Select this checkbox to Quarantine attachments that have not been scanned for malware infection.

Attachments Excluded (Whitelist)

The attachments added to this list will be excluded and not scanned for any viruses. This list is empty by default, it will allow you to add file names and file extensions that should not be blocked by MailScan. You can define the settings to allow specific files even if the file type is of the blocked category. In this case, suppose you have listed a particular file type to be blocked, you will have to specify the entire file name to be allowed. For example, if you have listed *.jpeg to be blocked, this will block all jpeg files. If you want to allow any specific jpeg file then enter the name of that file (name.jpeg); this will only allow the name.jpeg file.

- **Add**: Enter the file name with the extension type and click **Add**; this file will be allowed even if it falls in the blocked category.
- **Delete**: Click **Delete** to remove a file extension from the list to file extensions to be blocked.

Action

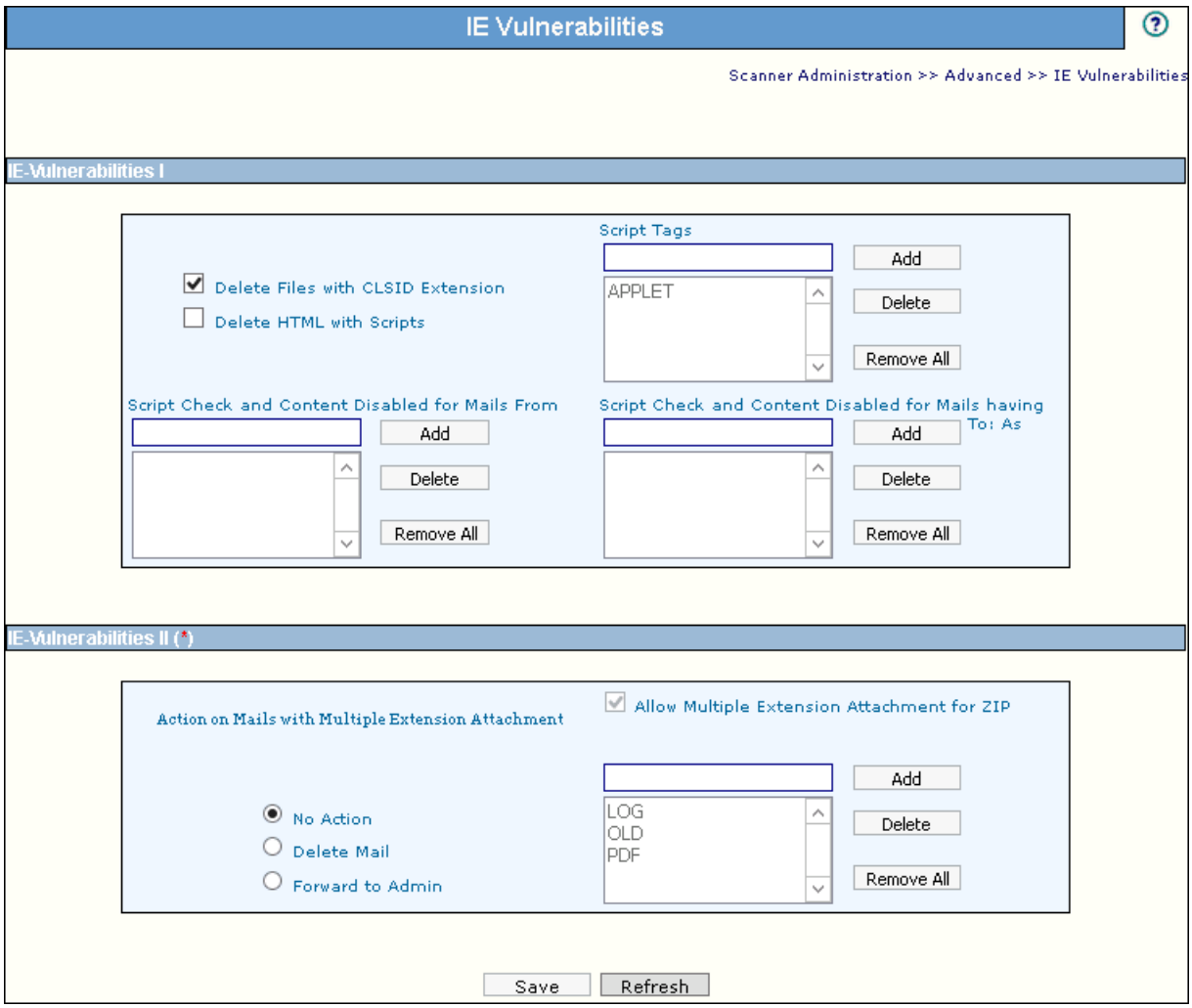
This will allow you to configure the action that MailScan should take whenever it detects an infected attachment. Learn more about Actions by clicking **here**.

Advanced

This will allow you to configure the advance settings for IE vulnerabilities and Archival.

IE vulnerabilities

This option will allow you to configure the settings for safeguarding emails from malware that exploit the vulnerabilities in the Internet Explorer. This page is divided into two sections IE vulnerabilities I and IE vulnerabilities II.



IE Vulnerabilities I

This section allows you to configure the settings that protect emails from malwares that use the browser's ability to support scripts.

- **Delete files with CLSID Extensions**: This check box is selected by default. Files with CLSID extensions are hidden files that do not show the actual file extension. If you select this option, MailScan deletes the attachments with CLSID file extensions to prevent dangerous files from exploiting the vulnerabilities in Internet Explorer.
- **Delete HTML attachments with Scripts**: Select this option to delete HTML attachments with embedded scripts. It will also allow you to specify the tags that MailScan should check for in the attachments so that the attachments containing those tags are deleted. By default, the Script Tags list, the Script and Content Check Disabled for Mails From list, and the Script and Content Check Disabled for Mails To list are disabled.
- **Script Tags**: It will display a list of script tags. MailScan will delete all email attachments in the HTML format containing the tags included in this list. It will also allow you to add tags to this list and MailScan will block HTML attachments that contain these tags.
    - **Add**: Enter the tag that you want to add to the Script tags list and click **Add**.
    - **Delete**: Select a tag from the Script tag list and click **Delete**; this will delete the tag from the scrip tag list.
    - **Remove All**: To clear the list, click **Remove All**.
- **Script Check and Content Disabled for Mails From**: This will allow you to add email IDs or domain names that you consider as legitimate senders. This feature of MailScan is useful when you want to receive legitimate emails in the HTML format with scripts. All emails in the HTML format with scripts coming from these users or domains are delivered to the inbox.
    - **Add**: Enter the email IDs or domain names that you consider as legitimate and click Add.
    - **Delete**: Click **Delete** to delete the selected email ID from the list of genuine sender email IDs or domain names.
    - **Remove All**: Click **Remove All** to remove all the email IDs or domain names from the list of sender email IDs or domain names.
- **Script check and content disabled for mails having To: As**: This will allow you to add email IDs or domain names that you consider as legitimate recipients. This feature of MailScan is useful when you want to send legitimate emails in the HTML format with scripts. All emails in the HTML format with scripts coming to these users or domains are delivered to the inbox.
    - **Add**: Enter the email IDs or domain names that you consider as legitimate and click **Add**.
    - **Delete**: Click this button to delete the selected email ID from the list of genuine recipients' email IDs or domain names.
    - **Remove All**: Click this button to delete all the email IDs or domain names from the list of recipient email IDs or domain names.

IE Vulnerabilities II

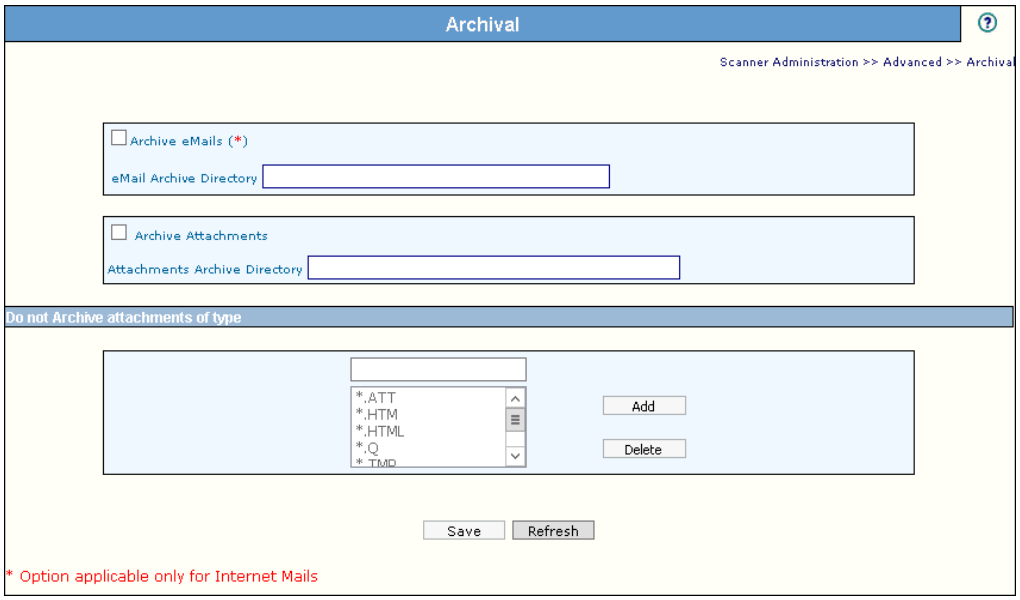
This will allow you to configure the actions that MailScan should perform on emails that contain attachments with multiple extensions.

- **Action on Mails with Multiple Extension Attachment**: This lets you configure MailScan to perform specific actions if attachments contain files with multiple extensions. You can configure MailScan to refrain from taking any action on the email, delete it, or forward it to the administrator.
    - **No Action**: If this option is selected, then MailScan will not take any action upon detecting an attachment with multiple extensions.
    - **Delete Mail**: If this option is selected, then MailScan will delete any attachment that has multiple extensions.
    - **Forward to Admin**: Select this option and MailScan will forward the attachment having multiple extensions to the administrator.
- **Allow Multiple Extension attachment for ZIP file**: Select this check box if you need MailScan to allow compressed files with multiple extensions as email attachments. The settings under Allow Multiple Extension attachment for ZIP file are disabled by default. They are enabled only when you select the Delete Mail option or the Forward to Admin option.
    - **Add**: You can click this button to add the file type specified in the box to the list.
    - **Delete**: You can click this button to delete the selected file type from the list.
    - **Remove All**: You can click this button to delete all the specified file types from the list.

To save all the settings, click **Save**. Click **Refresh** to refresh the interface.

Archival

This section lets you configure settings for archiving emails and attachments.

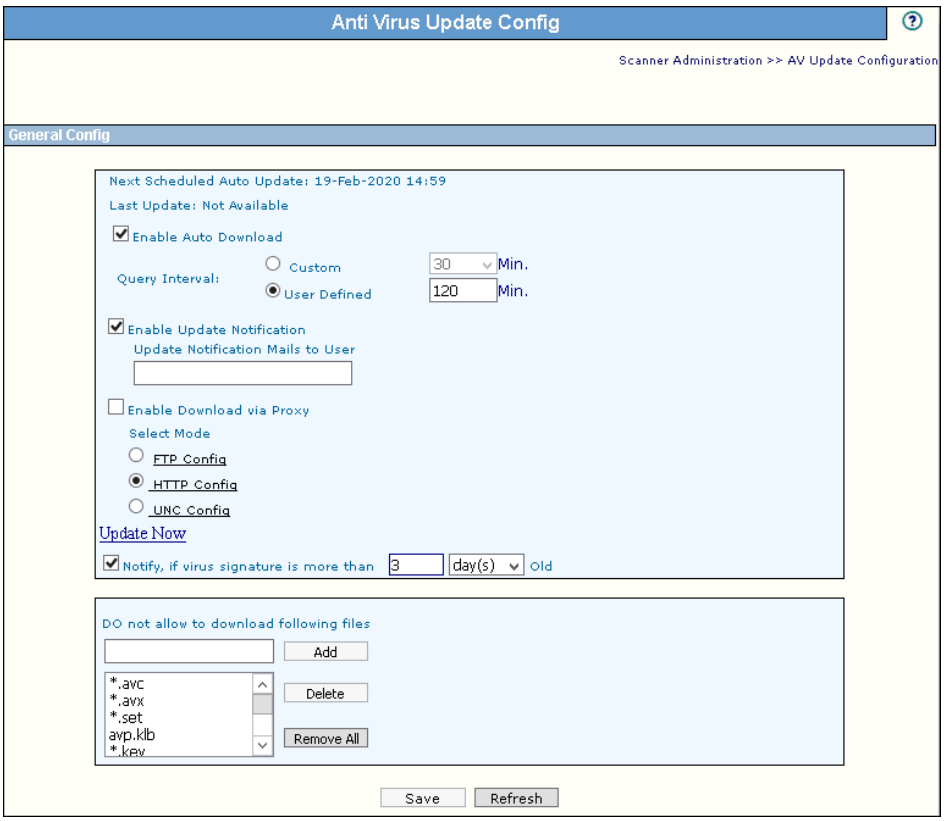


- **Archive emails (*)**: This option lets you archive or back up all emails that you have sent or received. MailScan provides you with the facility of backing up your emails to a given folder. The email Archive Directory box is disabled by default. Therefore, to specify the path of the backup folder, you need to select the Archive emails check box.
    - **Email Archive Directory**: It will display the path of the email Archive Directory; it will also allow you to write a different folder path for keeping the backup of all your emails.
- Archive Attachments: Select this check box if you need to archive or back up all sent or received email attachments to a given folder.
  However, to specify the path of the backup folder, you need to select the Archive Attachments check box because the Attachments Archive Directory box is disabled by default.
    - **Attachments Archive Directory**: It will display the path of the Attachments archived. It also lets you select a different folder path for keeping the email attachments.
- **Do not Archive attachments of type**: This will allow you to add attachment file types that you may not require to archive. You can exclude certain file types, such as *.VCF, *.HTM, and *.HTML, from being archived by adding them to the Do not Archive attachments of type list.
    - **Add**: You can click this button to add a file name or file type to the Do not Archive attachments of type list.
    - **Delete**: You can click this button to add a file name or file type to the Do not Archive attachments of type list.

To save all the settings, click **Save**. Click **Refresh** to refresh the interface.

AV Update Configuration

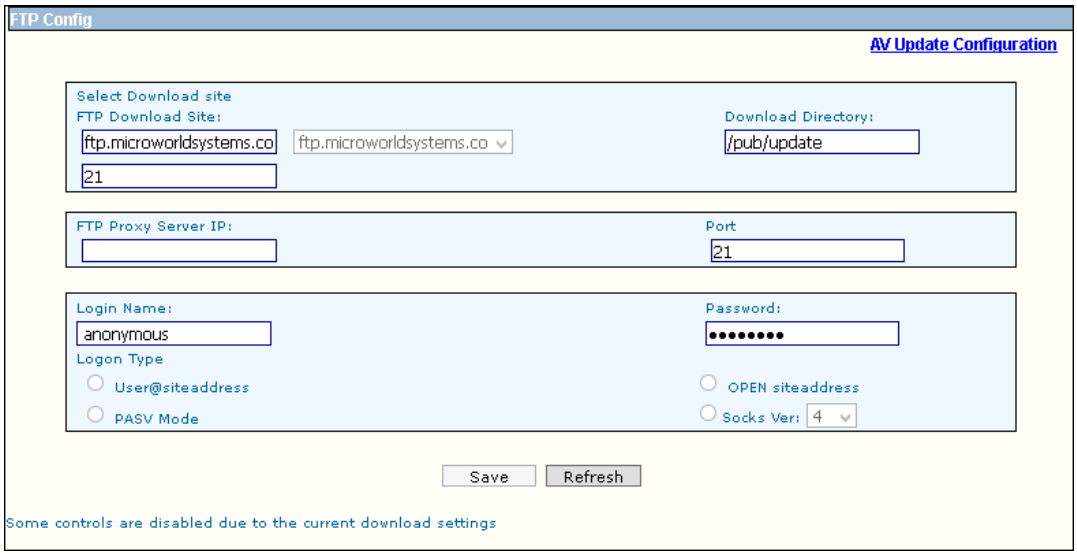
This option allows you to configure settings for downloading MailScan updates.



Administrator can define following settings for scheduling or manually downloading updates for MailScan:

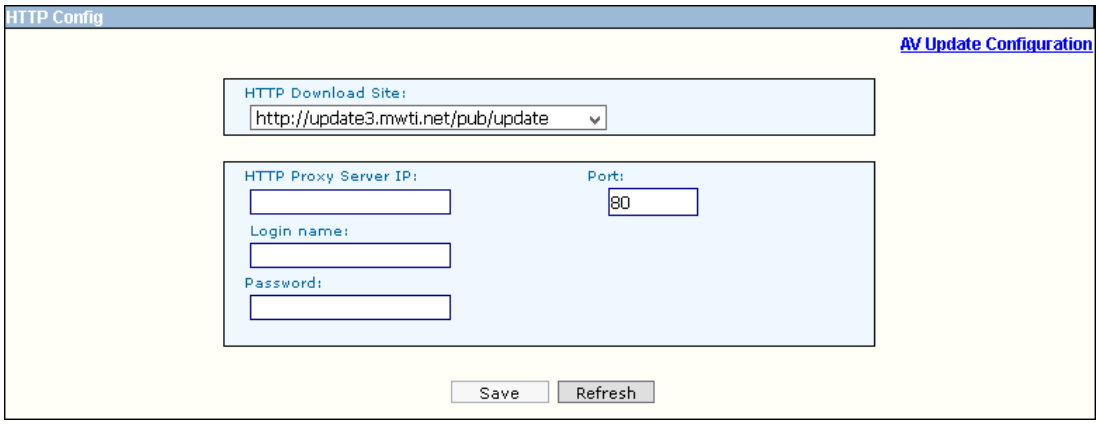
- **Enable Auto Download**: Select this option to enable the auto download of update. This option automatically downloads the update patches whenever they are released. You can define **Query Interval** for automatically checking the availability of updates on internet. MailScan gives you **Custom** as well as **User-Defined** to set the interval time.
  To set pre-defined time interval, follow the steps below:
  1. Select **Enable Auto Download** checkbox.
  2. Select **Custom** and select the desired time interval using the dropdown option.
  3. Click on the **Save** button present at the bottom of the interface.
- **Enable Update Notification**: This option allows you to define email address for sending email notification after every update. For enabling the update notification, follow the below steps:
  1. Select **Enable Update Notification** checkbox.
  2. Enter email address where the notification will be sent.
  3. Click on the **Save** button present at the bottom of the interface.
- **Enable Download via Proxy**: Select this option to enable download via proxy. MailScan allows you to select mode (**FTP Config**, **HTTP Config**, and **UNC Config**) and define the respective settings for downloading updates.

- **Configuring FTP option**
  Select **FTP Config** radio button and click on it. FTP Config window appears.



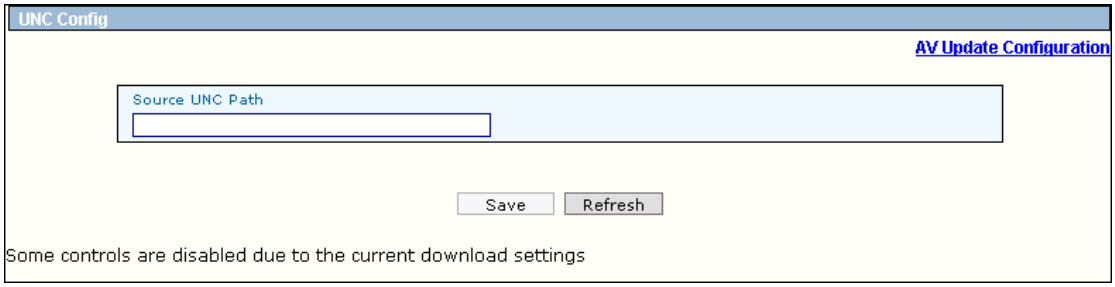
Enter FTP download site link along with Port number to download update. Enter the path where the updates will be downloaded in the respective fields. The sites are defined in the software and displayed in the dropdown list. Select the appropriate FTP site from the dropdown list. The application connects to this site to download updates. The ftp.microworldsystems.com is the default site. 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.
Enter the IP address of the computer along with port number where the proxy server will listen for FTP requests. In case authentication is required, fill in the mandatory login credentials. Click **Save.**

- **Configuring HTTP option**
  Select **HTTP Config** radio button and click on it. HTTP Config window appears.



  MailScan allows you to download updates through HTTP servers. Using this screen you can define http address as well as proxy server IP and port number along with credentials for authentication. Click **Save** to save the defined configuration settings.

- **Configuring UNC option**
  Select **UNC Config** radio button and click on it. UNC Config window appears.



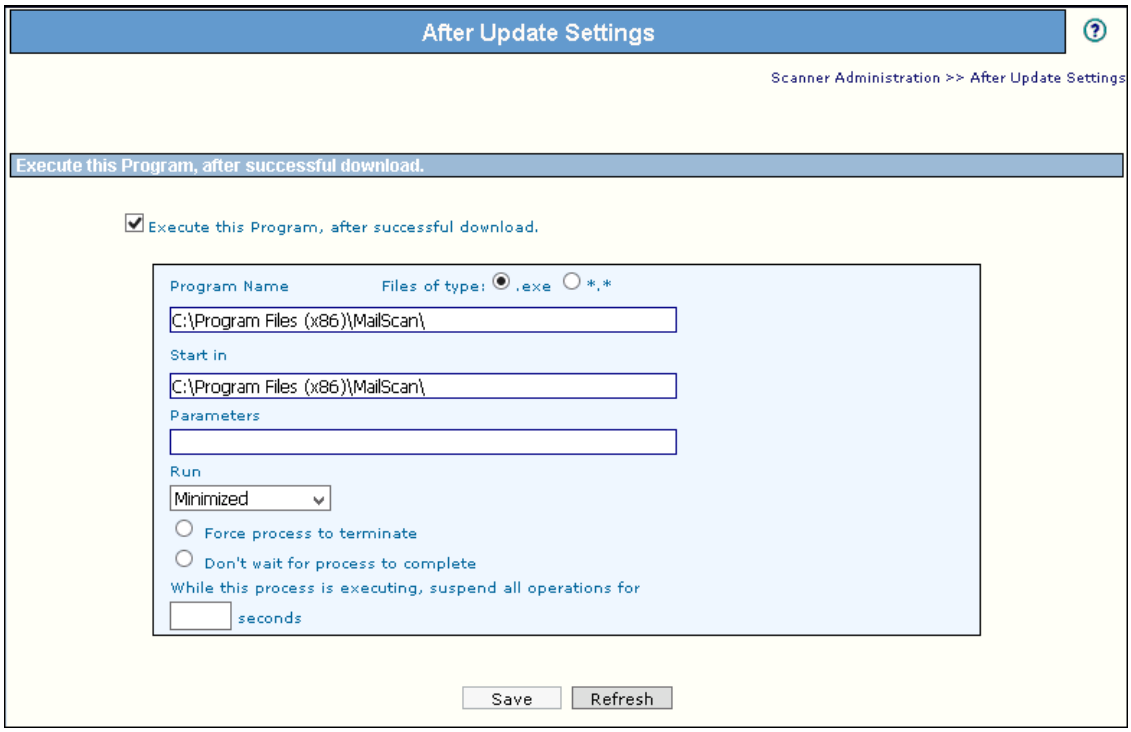
  Define the **Source UNC Path** where download patches have been kept on your system. MailScan will automatically install patches from the path for every update.

Note	In case if one mode is not working then the download will take place through another mode.

- **Update Now**: This option allows you to download virus pattern update manually from internet. Select **Notify, if virus signature is more than** checkbox to define the time interval. After you set the time interval, MailScan will notify you, in case there is an updated virus pattern.
- **Define and restrict file types from download**: This option allows you to define and restrict file extensions from being downloaded if received as attachments. It allows you to add desired file type or delete any existing file type from the restricted file extension list.

After Update Settings

This option lets you configure the action that MailScan performs after the updates are downloaded.



Execute this program, after successful download

Execute this program, after successful download: Select this checkbox to run a particular application or program after MailScan updates are downloaded successfully.

- **Program Name**: Specify the path of the program in the Program Name box. Sometimes, you may need a particular program to run after you have downloaded updates for MailScan.
- **Files of type**: This section lets you specify the type of file you can execute.
    - **.exe**: Select this option if you want MailScan to run only executable files after downloading updates.
    - ***.***: Select this option if you want MailScan to run all types of files after downloading updates.
- **Start in**: Specify the location of the folder where the program should execute.
- **Parameters**: specify the start parameters in the Parameters box as some programs require additional parameters to execute.
- **Run**: Specify whether the window should be in the maximized, minimized, normal, or hidden state. The default state of the window is normal.

- **Force process to terminate**: Select this option to forcibly terminate the process to free system resources.
- **Don't wait for process to complete**: Select this option to allow other processes to run along with the specified process as some process may require a long time to end.
- **While this process is executing, suspend all operations for __seconds**: Set a time limit and all other process will be suspended while the specified process is running.

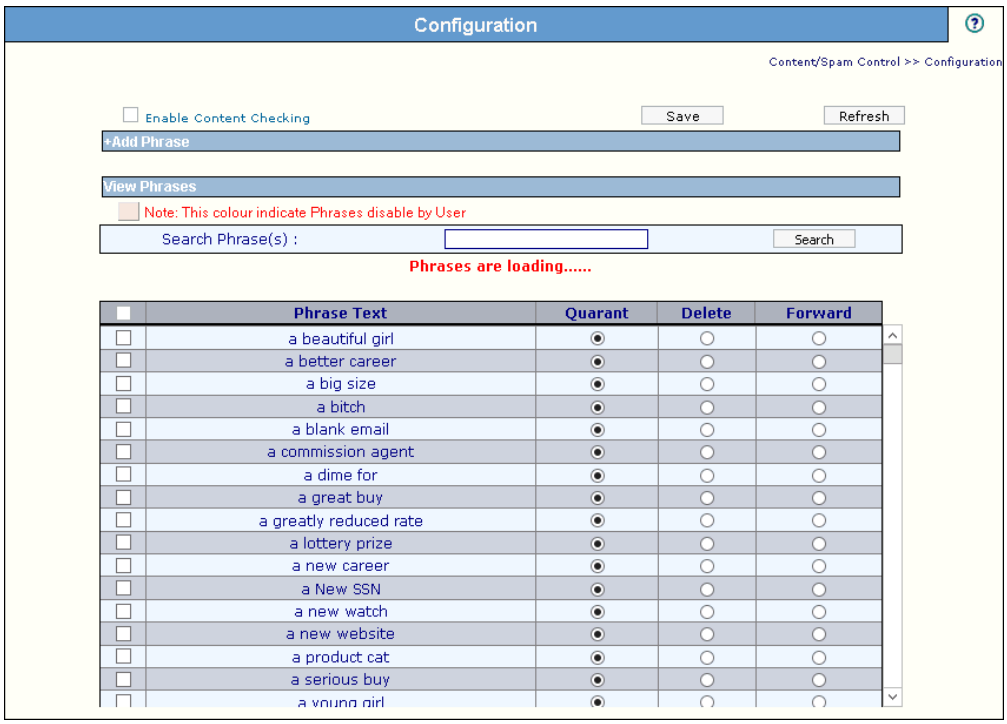
After you are done with the changes, click **Save**. Click **Refresh** to refresh the interface.

Content/Spam Control

This option lets you configure the settings for blocking and controlling spam and objectionable content in emails.

Configuration

This setting allows to enable content checking, based on phrases that are part of the content received in email. It allows you to define phrases and action that should be taken if email containing the defined phrases is received.



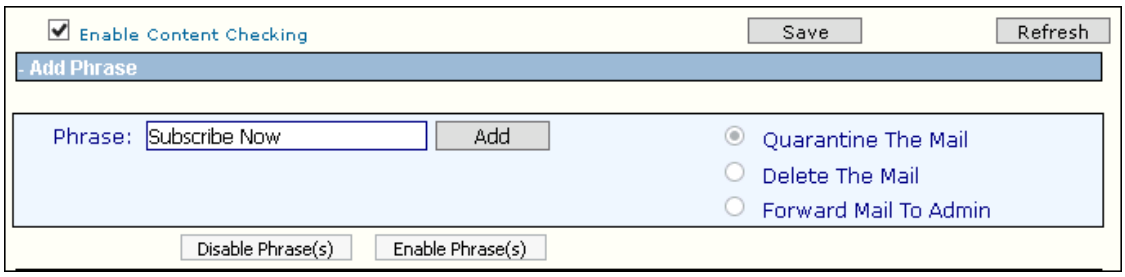
Configuring Content and Spam Control

Adding desired phrases:

To add desired phrases for blocking emails containing the added phrases, follow the below steps:

1. Select **Enable Content Checking** checkbox.
2. Click icon, you will get **Add Phrase** option.
3. Enter the phrase and select the actions to be performed. Following is the list of actions that can be defined through this module:
    - **Quarantine The Mail**: If the added phrase is present in the email, the email will be quarantined on receipt by MailScan.
    - **Delete The Mail**: If the added phrase is present in the email, the email will be deleted on receipt by MailScan.
    - **Forward Mail To Admin**: If the added phrase is present in the email, the email will be forwarded to Administrator on receipt by MailScan.

You can select enable or disable the phrases that are added.

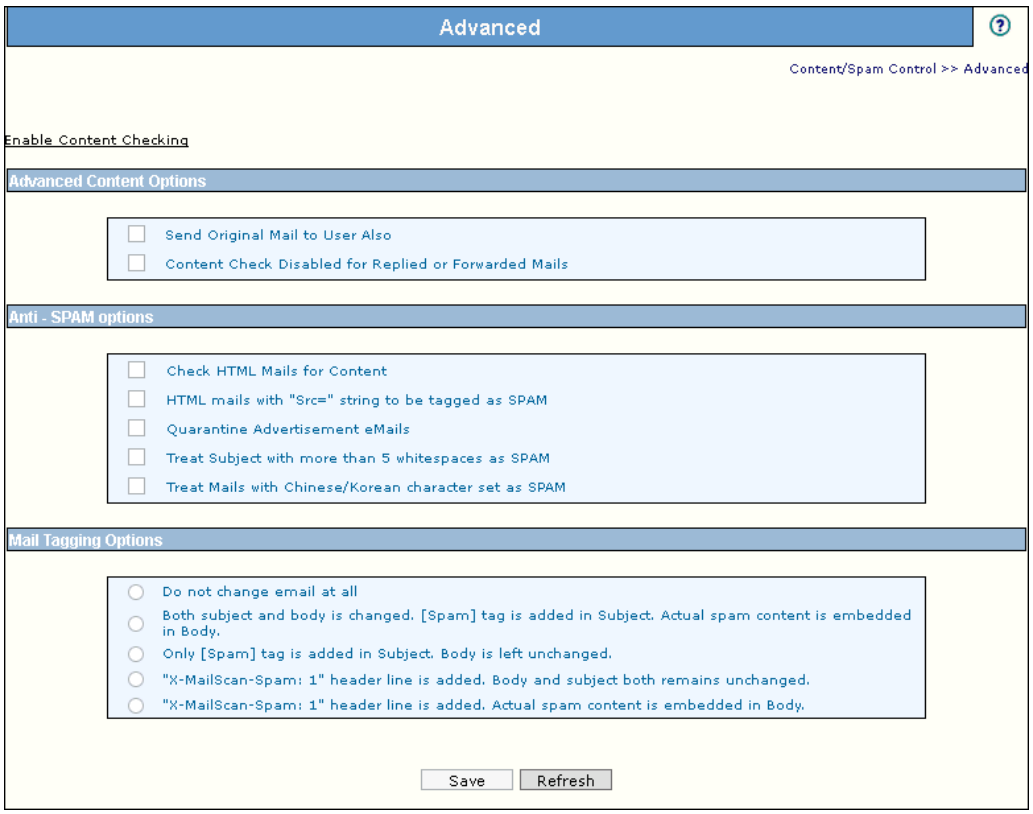


4. After providing the above details, click **Add**. The phrase will be added in the checklist and configured actions will be taken whenever an email is received with defined phrase.
5. Click **Save** to save the defined configuration setting.
6. Click **Refresh** to refresh the whole interface.

Searching Phrase(s): This option allows to search for phrases. You can sort the phrases in ascending or descending order.

Advanced

This will allow you to configure the general email options, spam filter, and mail tagging options available in MailScan.



Advanced Content Options

This section lets you configure the advanced content settings.

- **Send Original Mail to User**: Select this checkbox if you want to send original email tagged as SPAM to the recipient as well. When an email is tagged as SPAM, it is moved to this folder.
- **Content Check Disabled for Replied or Forwarded Mails**: Select this checkbox to ensure that MailScan does not check the contents of emails that the users have either replied or forwarded to other recipients.

Anti-Spam Options

This section will provide you with options for configuring the spam filter.

- **Check HTML Mails for Content**: Select this check box to scan emails in HTML format along with text content.
- **HTML mails with "Src=" string to be tagged as SPAM**: Select this checkbox to consider emails containing such strings as spam. HTML mails sent by spammers usually have links to banned images or URLs. These links are enclosed within the SRC string.
  For example, an email containing the code <td><img src="http://clicks.[xxxx].com/images/email/emm/hw/spacer.gif" width="302" height="1" border="0"></td> will be considered as spam because it contain the "Src=" string.
- **Quarantine Advertisement emails**: Select this option to check for advertisement mails and quarantine them.
- **Treat Subject with more than 5 whitespaces as SPAM**: [Default] Select this option to check the spacing between characters or words in the subject line of emails and treat emails with more than five whitespaces in their subject lines as spam emails. (MicroWorld in its research, found that spam emails usually contain more than five consecutive white spaces.)
- **Treat Mails with Chinese/Korean character set as SPAM**: [Default] Select this option to scan emails with the Chinese or Korean characters. This check is based on the research data conducted by MicroWorld's various spam email samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their emails.

Mail Tagging Options

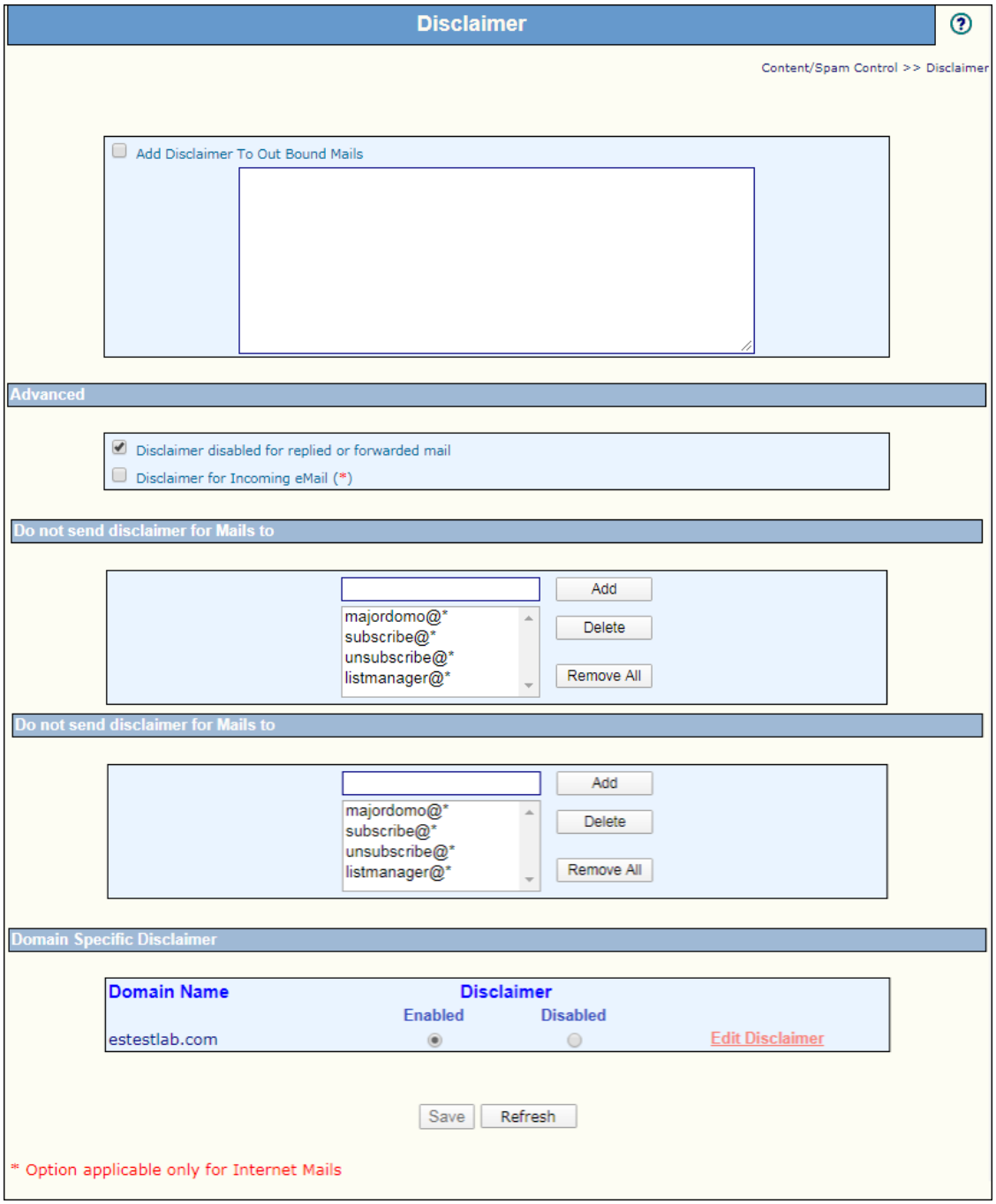
This section allows you to configure the settings for tagging emails that have been identified as spam.

- **Do not change email at all**:
  Select this checkbox to prevent Anti-Spam from adding the [Spam] tag to emails that have been identified as spam.
- **Both subject and body are changed. [Spam] tag is added in Subject: Actual spam content is embedded in Body**:
  Select this checkbox to help you add the [Spam] tag only in the body of the email that has been identified as spam.
- **Only [Spam] tag is added in Subject. Body is left unchanged**:
  Select this checkbox to add the [Spam] tag only in the subject of the email that has been identified as spam.
- **X-MailScan-Spam: 1" header line is added**: **Body and subject both remain unchanged**:
  [Default] Select this checkbox to add a header line to the email. However, this does not add any tag to the subject-line or body of the email.
- **X-MailScan-Spam: 1" header line is added: Actual spam content is embedded in Body**: Select this option to add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.

Click on **Save** button to save the defined configuration settings. Click **Refresh** to refresh the interface.

Disclaimer

This submodule lets you configure settings related to adding a disclaimer to emails. You can add customized disclaimers to both incoming and outgoing emails.



Add Disclaimer To Out Bound Mails: Select this checkbox to add a disclaimer to all outgoing emails. The disclaimer notifies recipient that the email is scanned and virus-free.

Advanced

This section lets you configure the Advanced Disclaimer settings.

- **Disclaimer disabled for replied or forwarded mail**: Select this option if you do not want MailScan to add a disclaimer to replied or forwarded emails.
- **Disclaimer for Incoming email ( )**: Select this option to add a disclaimer to incoming emails. This is applicable only to the emails received from the Internet.

Do not send disclaimer for Mails to

This section lets you add the email IDs of recipients. MailScan will not add a disclaimer to the emails sent to the recipients in this list.

- **Add**: Enter the recipient's email ID and click **Add**. The recipients will be added.
- **Delete**: Select a recipient from the list and then click **Delete**.
- **Remove All**: To remove all the recipients from the list, click **Remove All**.

Domain Specific Disclaimer

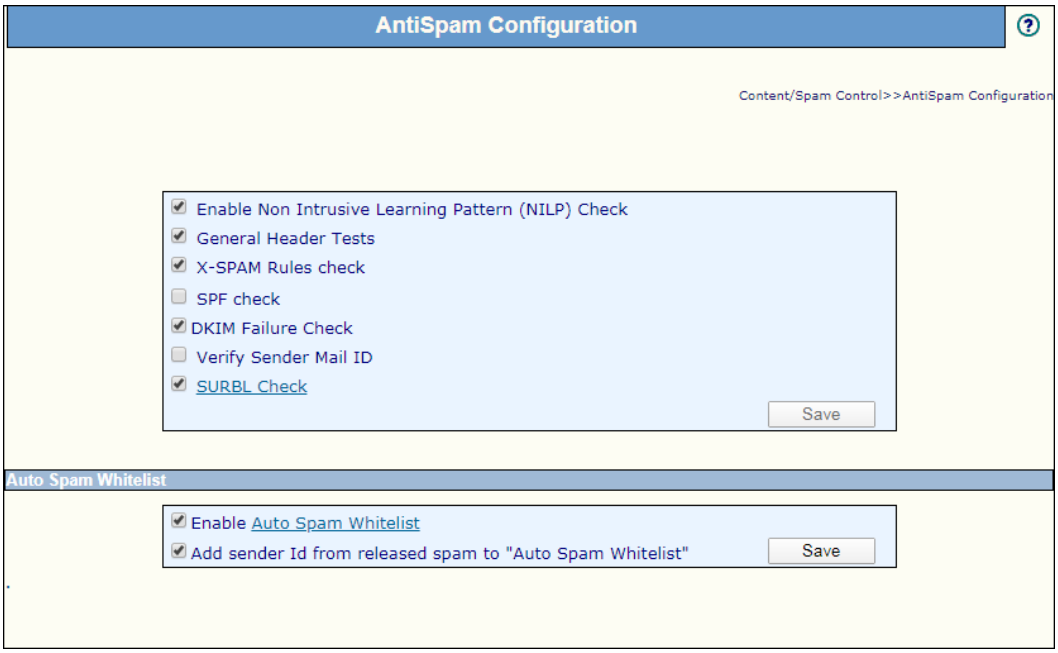
This will allow you to add customized disclaimers to emails sent to local domains. This section lets you configure the domain specific disclaimer settings.

- **Domain Name**: This column lists the local domains on the network.
- **Disclaimer:** This section lets you enable or disable the domain specific disclaimer for the corresponding domain.
    - **Enabled**: Select this option if you want to add a customized disclaimer to the emails sent to the corresponding local domain.
    - **Disabled**: Select this option if you do not want to add a customized disclaimer to the emails sent to the corresponding local domain.
- **Edit Disclaimer**: Click this link to edit the disclaimer settings for the corresponding local domain. When you click this link, the following webpage is displayed.

Click on **Save** to save the configuration. Click **Refresh** to refresh the interface.

Antispam Configuration

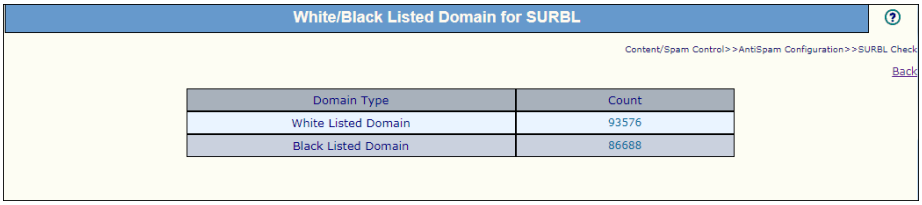
This submodule lets you configure the settings for the Anti-Spam feature of MailScan.



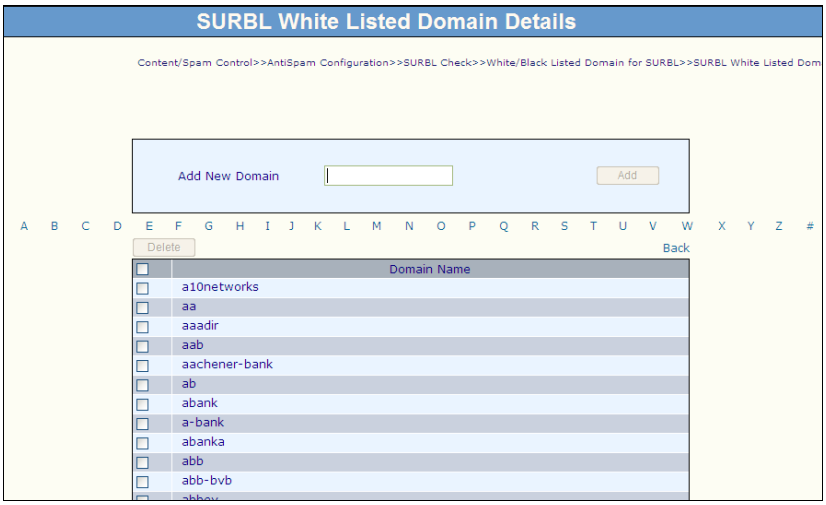
This section contains the general settings for configuring the Anti-Spam module of MailScan.

- **Enable Non-Intrusive Learning Pattern (NILP) Check**: Select this checkbox if you want MailScan to check emails by using the NILP technology.
  NILP is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each email and prevents spam emails and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user.
- **General Header Tests**: [Default] Select this option to check the validity of certain generic boxes like From ID, To ID, CC ID in emails and mark them as spam if any of the headers are invalid.
- **X-SPAM Rules check**: [Default] Select this option to check whether the emails confirm to XSPAM rules or not. X-SPAM Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in MailScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The SPAM Rules Check will match the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. The Anti-Spam module of MailScan refers to this database to identify emails and takes actions on them.
- **SPF check**: SPF (Sender Policy Framework) is a world standard framework adopted by MailScan to prevent hackers from forging sender addresses. It acts as a powerful mechanism for controlling phishing mails. Select this option to check the SPF record of the sender domain.
- **DKIM Failure Check**: [Default] This option will check all incoming emails from foreign domain for valid DKIM signature. Emails with invalid DKIM signature will be quarantined.

- **Verify Sender Mail ID**: Select this checkbox to verify the authenticity of sender's email ID and its domain.
- **SURBL check**: [Default] Select this option to check the URLs in the body of an email. If the URL is listed in the SURBL site, the email will be blocked. This option requires Internet connectivity for best results. You can click this link to view the White/Blacklisted Domains for SURBL page that displays the number of whitelisted or blacklisted domains.



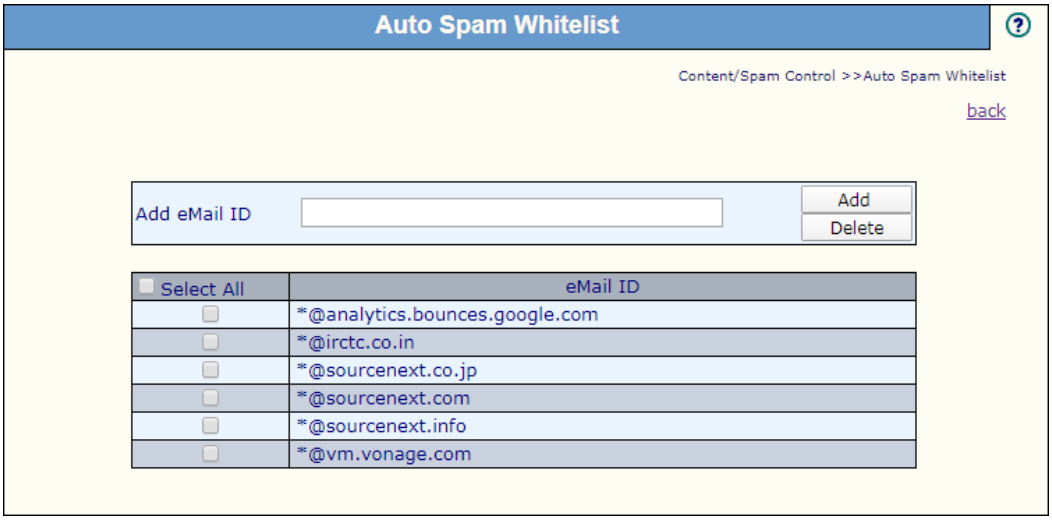
  - **Domain Type**: This column displays the type of domain, whether it is whitelisted or blacklisted.
  - **Count**: This column displays the number of domains listed for that domain type. You can click the number listed in this column to view a page that displays the list of domains belonging to the corresponding domain type.



    - **Add New Domain**: Enter the domain name to be added to the list.
    - **Add**: Click **Add** to add the domain specified in **the Add New Domain** box to the list of domains.
    - **Delete**: To delete a domain from the list, select a domain and click **Delete**.

Auto Spam Whitelist

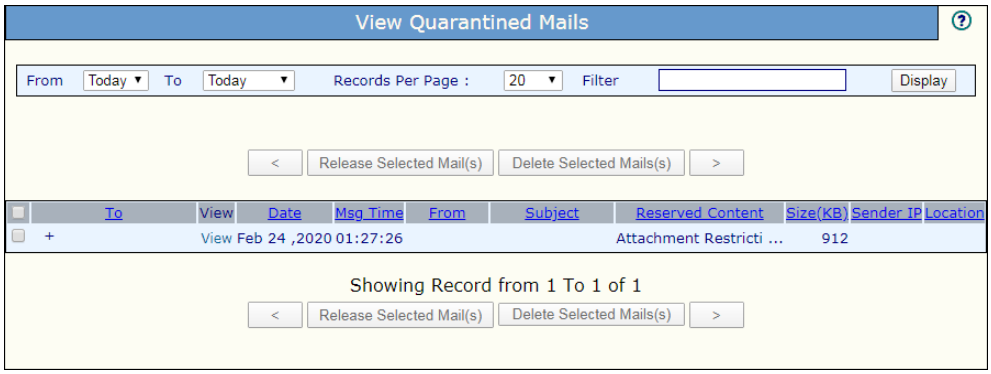
The Auto Spam Whitelist contains a list of valid email IDs that can bypass the above spam filtering options. When a local user sends an email to an email address, the system automatically adds that ID to the Spam Whitelist. In addition, this feature allows you to specify email ID of senders that you want to exclude from all Spam filtering. It thus allows emails from the whitelisted ids to be downloaded to the recipient's inbox. The Auto Spam Whitelist contains a list of valid email IDs that can bypass the above spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox.



Add email ID: To add an email ID, enter the email ID and click **Add**.
Delete: To delete an email ID, select the email ID from the list and click **Delete**.

Quarantined Mails

This page will display the emails that have been quarantined by MailScan.



From/To lists: Select a specific range of dates by selecting the start date and end date from the From and To drop down lists.
Records Per Page: Select the number of emails that should be displayed on this page by selecting a value from this list.
Filter: Specify keyword(s) in this box and display the emails that match the search criterion.
The boxes in the table: The table displays the following boxes.

- **To**: This column displays the email ID of the recipient.
- **View**: Click on this link to view the details as well as content of the email being sent.
- **Date**: This column displays the date on which the email was received.
- **Msg Time**: This column displays the time when the email message was received.
- **From**: This column displays the email ID of the sender.
- **Subject**: This column displays the subject of the email.
- **Reserved Content**: This column displays whether the email content had any reserved content. Or will display the reasons why the email is considered SPAM.
- **Size (KB)**: This column displays the size of the email in KB.
- **Sender IP**: This column will display the IP address of the sender.
- **Location**: This column will display the location of the sender.

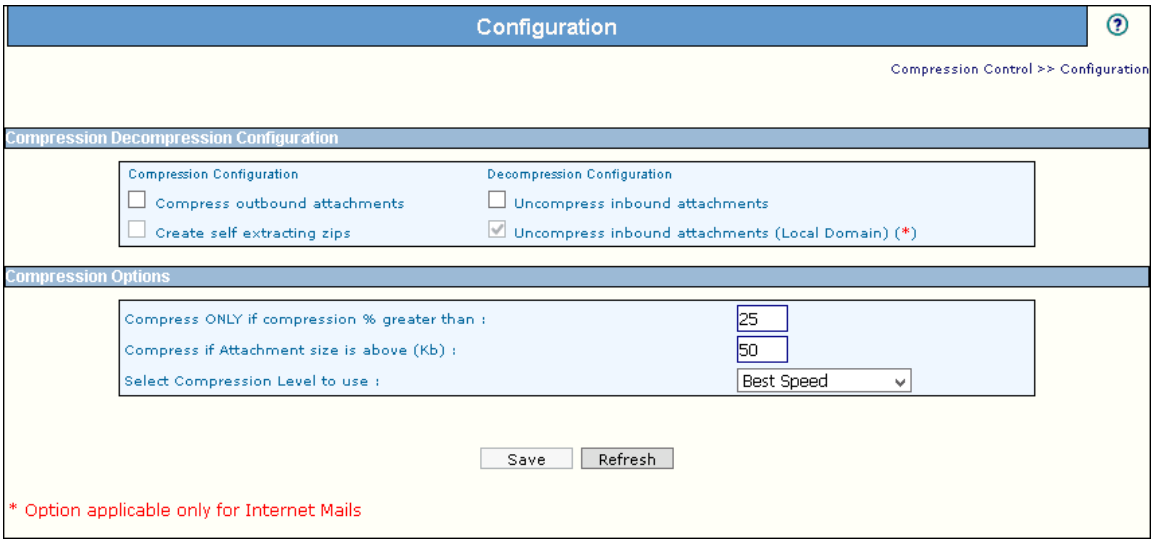
It also allows you to select and release email from the Quarantined folder or Delete it if desired.

Compression Control

Auto-compression of attachments is a feature that allows automatic compression of Outgoing and Incoming attachments. The Compression Control section lets you configure the settings for compressing or decompressing email attachments.

Configuration

This setting allows to auto-compression of incoming and outgoing attachments. In this section, you can configure the setting for compressing or decompressing the email attachments.



Configuring Compression Control

- **Compression Decompression Configuration**:
  This section will allow you to define the compression and decompression configuration.

  (Compression Configuration)
  - **Compress outbound attachments**: Enable this checkbox to auto compress the attachments of outgoing emails.
  - **Create self extracting zips**: Enable this check box to create self-extracting ZIP files of outgoing email attachments. This option is useful when the recipient does not have the software to unzip the attachments. This field is enabled only if **Compress outbound attachments** check box is selected.

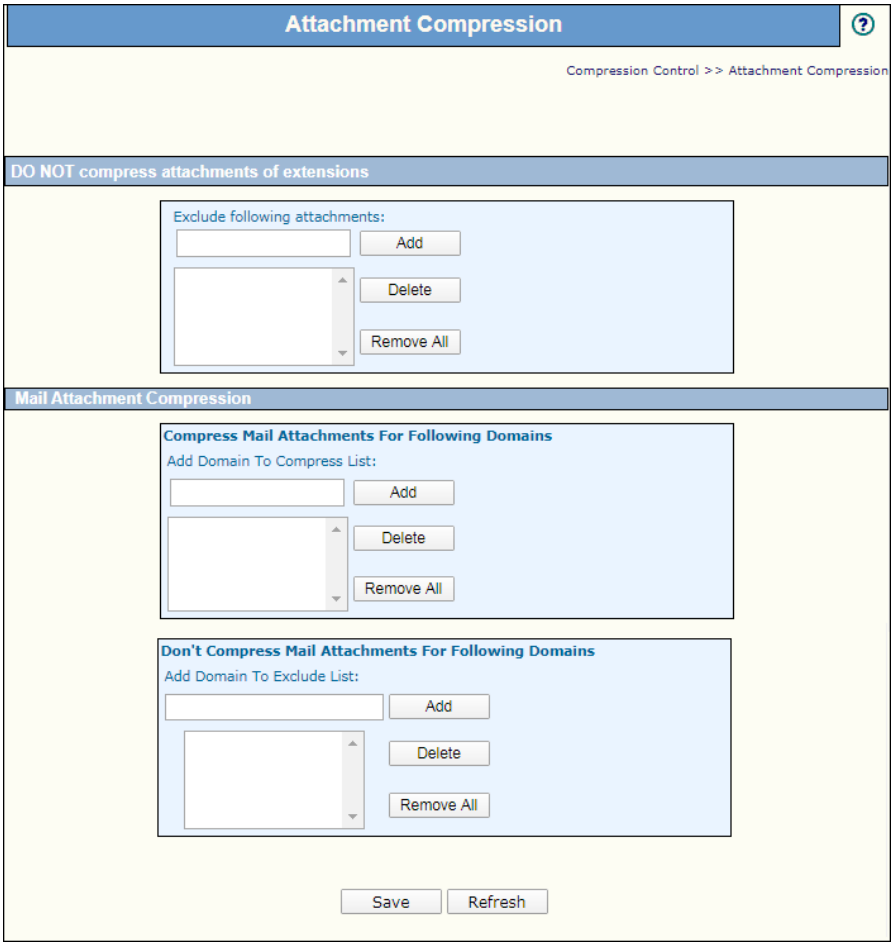
  (Decompression Configuration)
  - **Uncompress inbound attachments**: Enable this checkbox to auto-decompress the attachments of incoming emails.
  - **Uncompress inbound attachments (Local Domains)**: Enable this option to decompress the incoming local email attachments. This is enabled by default.

- **Compression Options**:
  - **Compress ONLY if compression % greater than**: Some files cannot be compressed beyond a limit. In this field, you can specify the minimum compression percentage. Any file, which cannot be compressed beyond the specified value, will not be compressed.
  - **Compress if the Attachment size is above (Kb)**: Define the size in KB for attachments; it will be compressed only if it exceeds the defined size.
  - **Select Compression Level to use**: Select the appropriate compression level from the following dropdown list:
    - **Default**: Ensures the optimum balance between speed and compression quality.
    - **Best Compression**: Ensures the maximum amount of compression but may take more time on a slower machine.
    - **Best Speed**: Ensures the best speed of compression. Quality of compression may not be optimized.

Click **Save** to save the configured setting and **Refresh** to refresh the interface.

Attachment Compression

This submodule lets you specify the compression configuration for the attachments.



DO NOT compress attachments of extensions

The type of attachments specified in this list will be excluded from auto-compression.

- **Exclude Following attachments**: Specify the type of attachments that should be excluded from auto-compression.
    - **Add**: Enter the type of attachment that needs to be excluded from auto-compression and click **Add**.
    - **Delete**: Select a file type and click **Delete** to remove the particular file type from the list.
    - **Remove All**: Click **Remove All** to remove all the files from the list of attachments.

Mail Attachment Compression

Compress Mail Attachments for Following Domains

This will allow you to specify the settings for compressing mails pertaining to certain domains.

- **Add Domain To Compress List**: The attachments from the domain names specified in this list will be compressed.
    - **Add**: Enter the domain name and click **Add**.
    - **Delete**: Select a Domain name and click **Delete**; this domain will be removed from the list.
    - **Remove All**: Click this to remove all the domains from the list.

Don't Compress Mail Attachments For Following Domains

The attachments from the domain names specified in this list will be excluded from compression.

- **Add Domain To Exclude List**: Specify the domain names for which the attachments are to be excluded from compression.
    - **Add**: To add a domain, enter the domain name and click **Add**.
    - **Delete**: To delete a domain, select a domain name and click **Delete**.
    - **Remove All**: To remove all domains from the list, click Remove All.

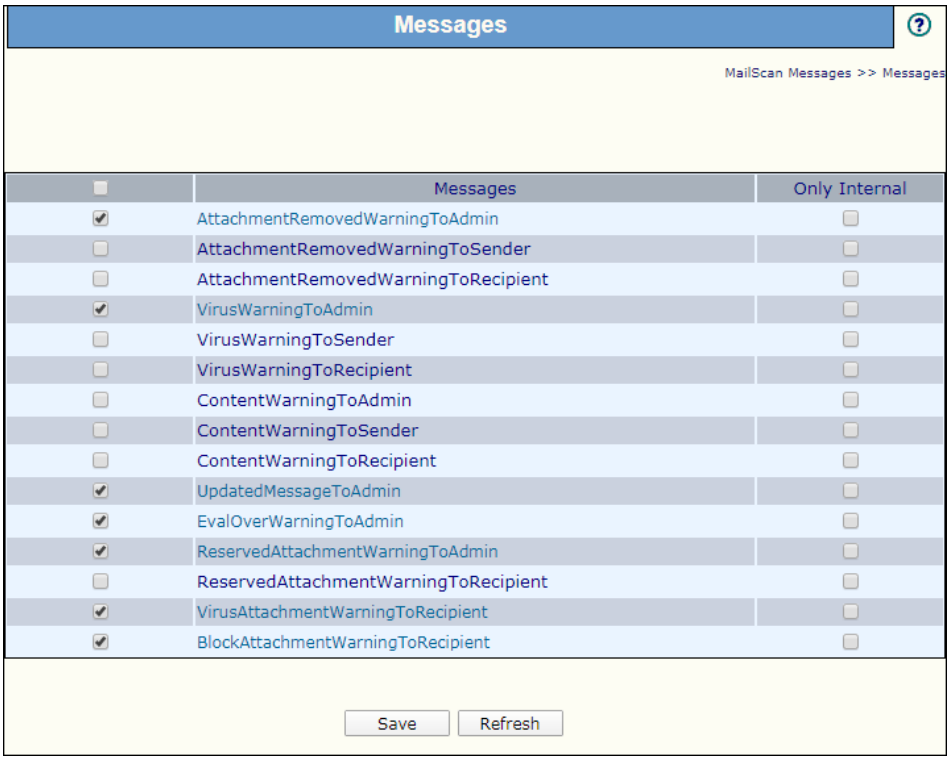
After you are done with the changes, click **Save**. Click **Refresh** to refresh the interface.

MailScan Messages

This Module allows you to select, define and configure settings for sending notification mails through MailScan on occurrence of security violation. Additionally, you can also configure settings for sending outbreak alerts.
A customized notification message can be sent to the sender, receiver, or others, informing them about the action taken.

Messages

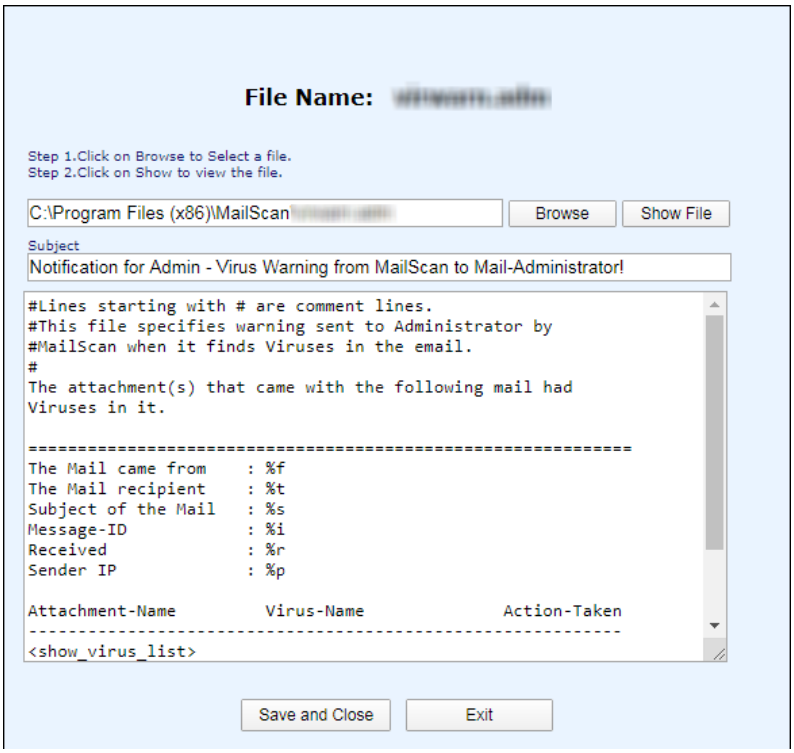
If MailScan detects a virus, malicious attachment, restricted words, or phrases that violate your organization's security policy, it informs you immediately and lets you delete, quarantine, or disinfect the specific email and attachment. You can also send a customized notification message to the sender, receiver, or administrator informing them about the action taken on infected/malicious email.



A list of warning messages will be displayed, select the checkbox on the left side and click **Save**.

Note	Select the **Only Internal** column checkbox to send the message only for internal mails.

Click the message title and a new pop-up window will be opened displaying the notification message.

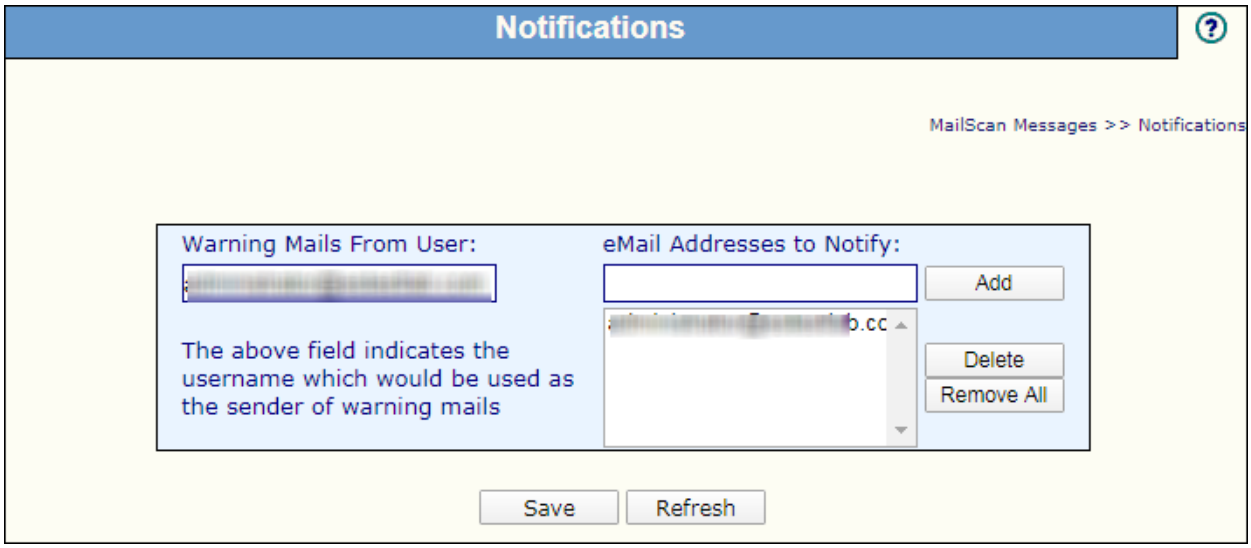


It also lets you customize the message. To save the message, click **Save and Close.**

Note	To view a message that is not a link; check the corresponding checkbox and click **Save** and the link will be formed.

Notifications

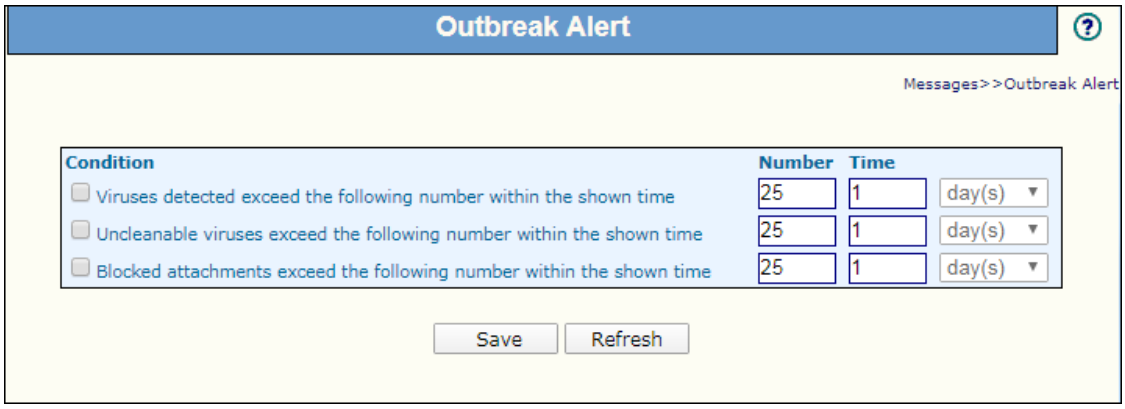
The Notifications submodule lets you configure the settings for sending customized notification messages to the sender, receiver, or others, informing them about the action taken on infected/malicious mail or attachment.



- **Add**: To add an email address, enter the email ID and click **Add**.
- **Delete**: To delete an email address, select an email ID and click **Delete**.
- **Remove All**: To remove all email IDs from the list, click **Remove All**.

Outbreak Alert

This submodule lets you configure the MailScan settings for performing specific actions when a virus outbreak occurs.



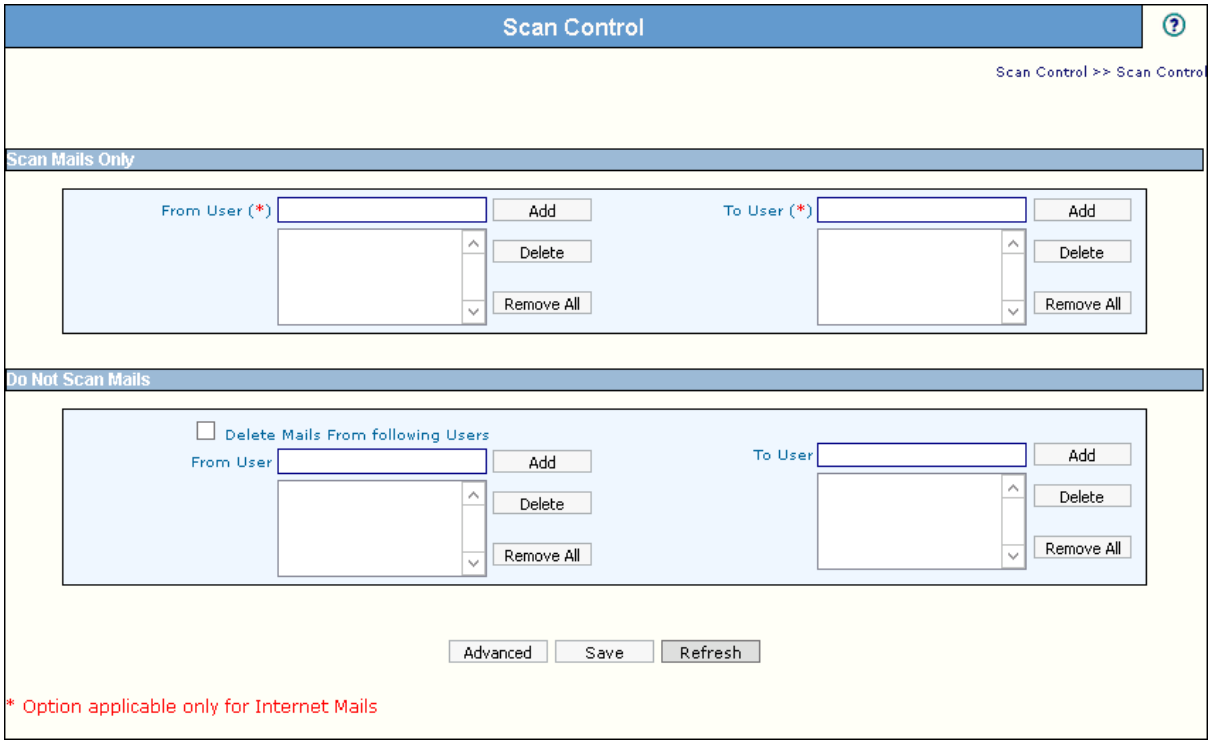
You can configure the settings for a situation to be declared as Virus Outbreak. Enter the number of viruses detected, time limit, and select the conditions as when it is to be declared as virus Outbreak. Using this module you can simply define the following.

- Number of Viruses detected and number of times it exceeds the defined count in a day.
- Un-cleanable virus count and number of times it exceeds the defined count in a day.
- Blocked attachments and number of time it exceeds in a day.

A notification mail will be sent to the administrator if any of the above condition matches.

Scan Control

This setting allows you to specify email IDs that should be scanned or exempted for virus scanning. You can also specify the email IDs that are to be deleted.



You can configure the following options:

Scan Mails Only

This option allows you to assign **From User** and **To User** emails to be scanned.

- **From User**: All the emails **From** the defined users are scanned.
- **To User**: All the emails **To** the defined users are scanned.
  Following are the options that are common for above both options:
  - **Add**: Enter the email address and click Add.
  - **Delete**: Select the email address and click **Delete**, this will delete the email address from the list.
  - **Remove All**: This will delete all the email address from the lists.

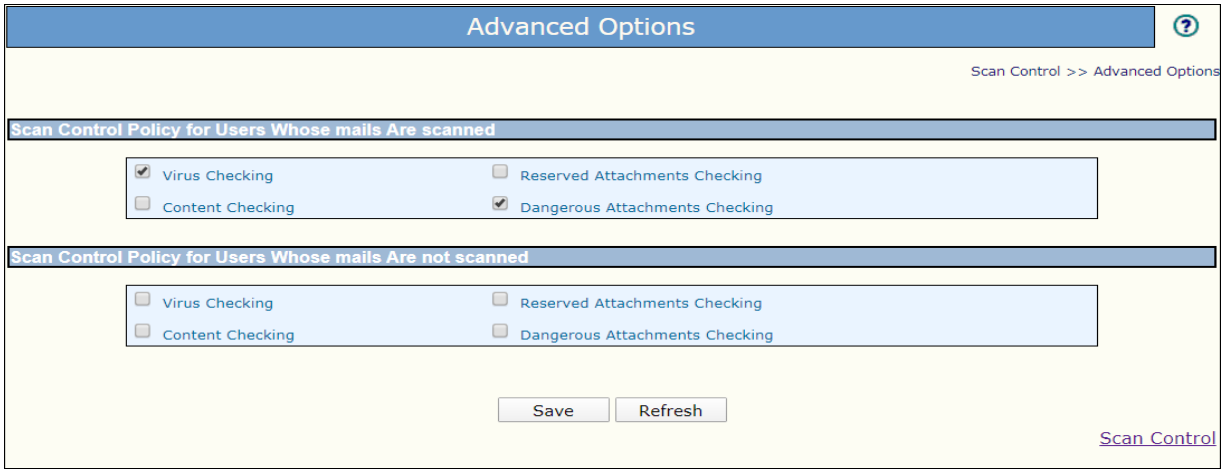
Do Not Scan Mails

This option will allow you to assign **From User** and **To User** email that need to be excluded from scanning. You can also delete the mails from the users added in the list.

- **Delete mails from the following users**: Select this check box to delete all the mails from the added users in the list.
    - **From User**: All the emails From the defined users are not scanned. In case the above option is enabled, then it will directly delete the emails **From** the listed users.
    - **To User**: All the emails To the defined users are not scanned. In case the above option is enabled, then it will directly delete the emails **To** the listed users.

Advanced

To configure the advanced options for scanning mails, click **Advanced**.
The **Advanced Options** lets you configure Scan Control Policy for users whose mails are scanned and users whose mails are not scanned.



Scan Control Policy for Users Whose mails Are scanned:

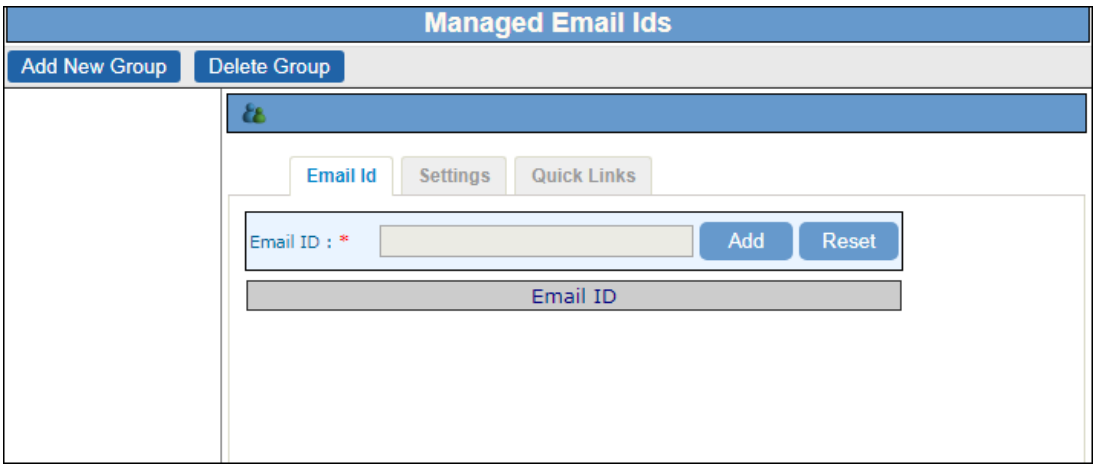
- **Virus Checking:** Select this check box to scan emails for viruses.
- **Reserved Attachments Checking:** Select this check box to scan restricted attachments.
- **Content Checking:** Select this check box to scan email contents for offensive words and phrases.
- **Dangerous Attachments Checking:** Select this check box to scan dangerous email attachments for virus. These are specified in To block/allow attachments.

Scan Control Policy for Users Whose mails Are not scanned:

- **Virus Checking:** Select this check box to scan emails for viruses, this option is disabled by default.
- **Reserved Attachments Checking:** Select this check box to scan restricted attachments.
- **Content Checking:** Select this check box to scan email contents for offensive words and phrases.
- **Dangerous Attachments Checking**: Select this check box to scan dangerous email attachments for virus. These are specified in To block/allow attachments.

Managed Email Ids

This module allows you to define groups and put email addresses in created groups and later define permissions and settings for the defined groups.



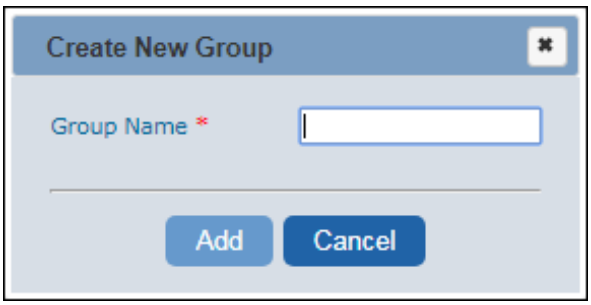
Email Id

This tab will allow to add and delete the groups according to the specific need.

Add New Group

To add a new group, follow the below steps:

1. Click on **Add New Group** present on the interface.

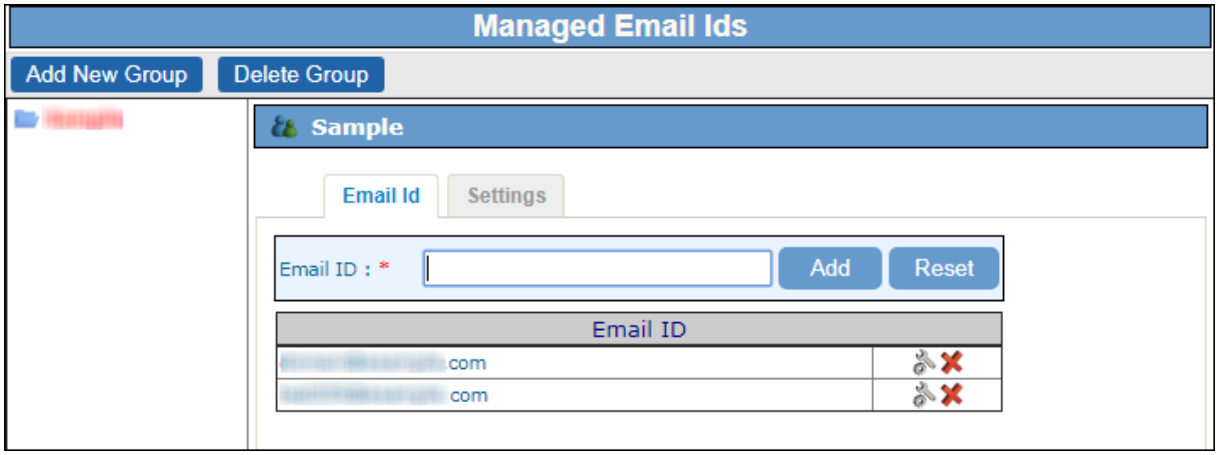


2. Enter the Name for the Group and click on **Add** button
3. The group will be added instantly.

Add email IDs to the Group

To add email addresses to the group, follow the below steps:

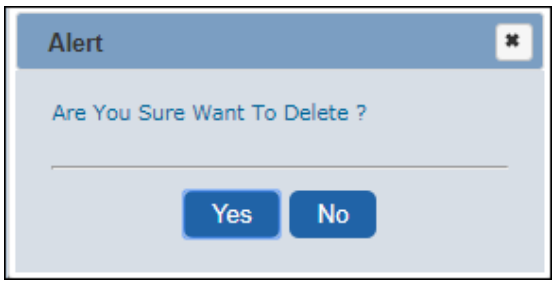
1. Select the desired group to add email addresses.
2. Enter the email address in the text area for **Email ID** and click on **Add** button.
3. The email address will be added instantly to the selected group.



Delete a Group

To delete a group, follow the below steps:

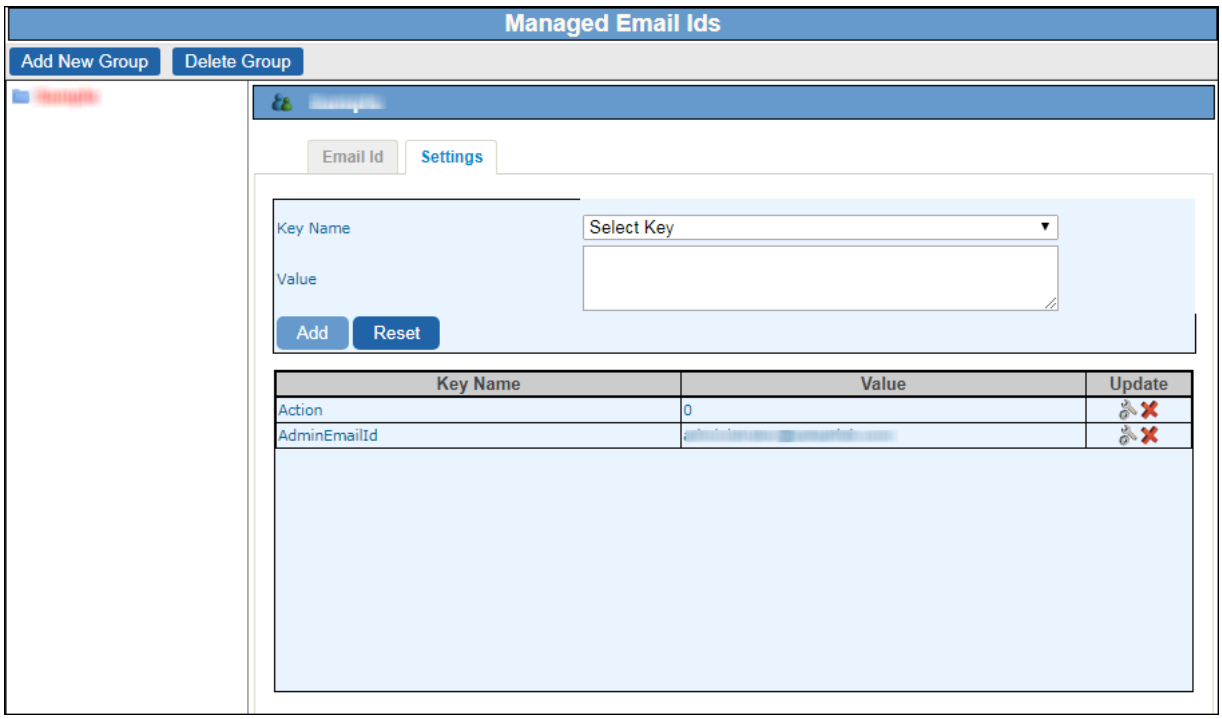
1. Select the group, you want to delete. Click **Delete**.



2. Click **Yes**. The group will be deleted.

Settings

Select the Group and go to **Settings** Tab, here you can define settings for the created group.



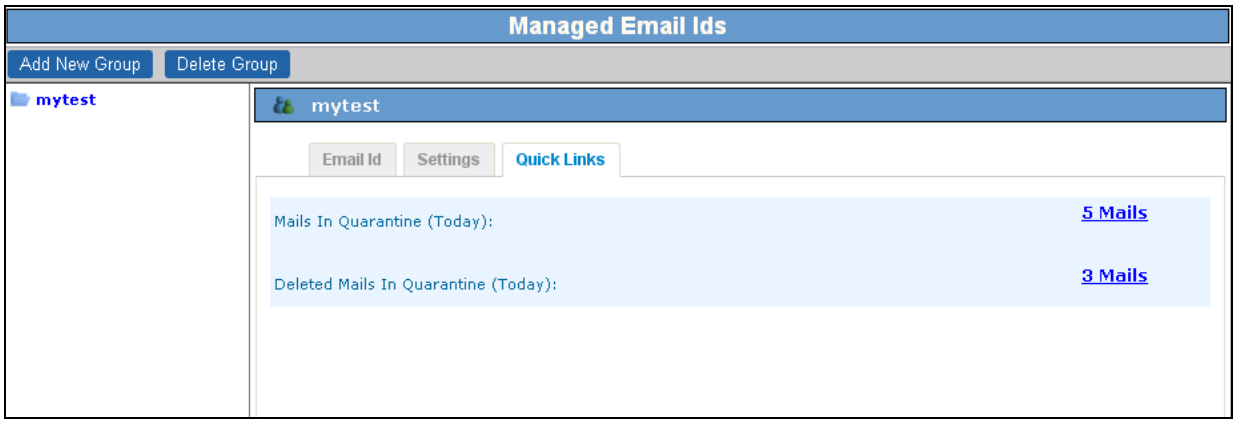
- **Key Name**: Use this dropdown to select and apply desired setting on the group.
- **Value**: This will Display / Allow you to enter Value / Parameter for the selected setting.
- **Add**: Click **Add** to Apply the Settings to the group, this also allows you to Add Select and Add multiple settings to the selected group.
- **Reset**: Click **Reset** to reset the configuration.

Note	You can Add multiple settings to the selected Group using the options present on the interface.

Once added the above defined settings will be implemented on all email addresses added/present in selected Group.

Quick Links

This tab will be visible only if you have selected Quarantine directory and defined path for storing mails quarantined for the group using the **Key Name** dropdown under **Settings** tab. It displays number of the mails quarantined as well as deleted in the group. For further details you can click on respective links present on the interface.

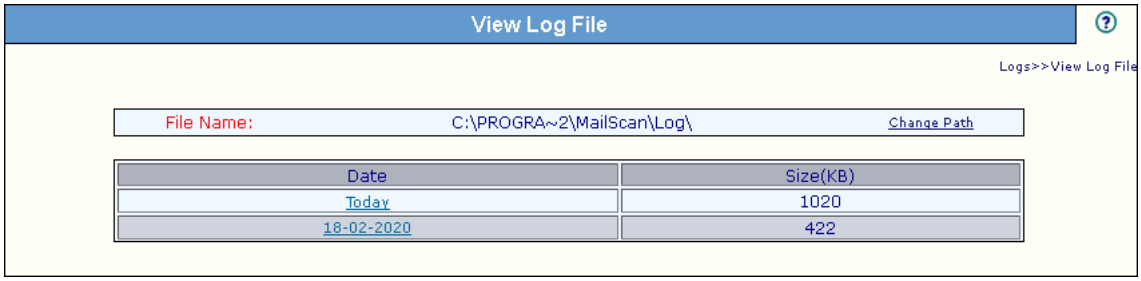


Logs

MailScan generates a variety of log files that gives system administrators an overview and detailed information of MailScan activity in the network.

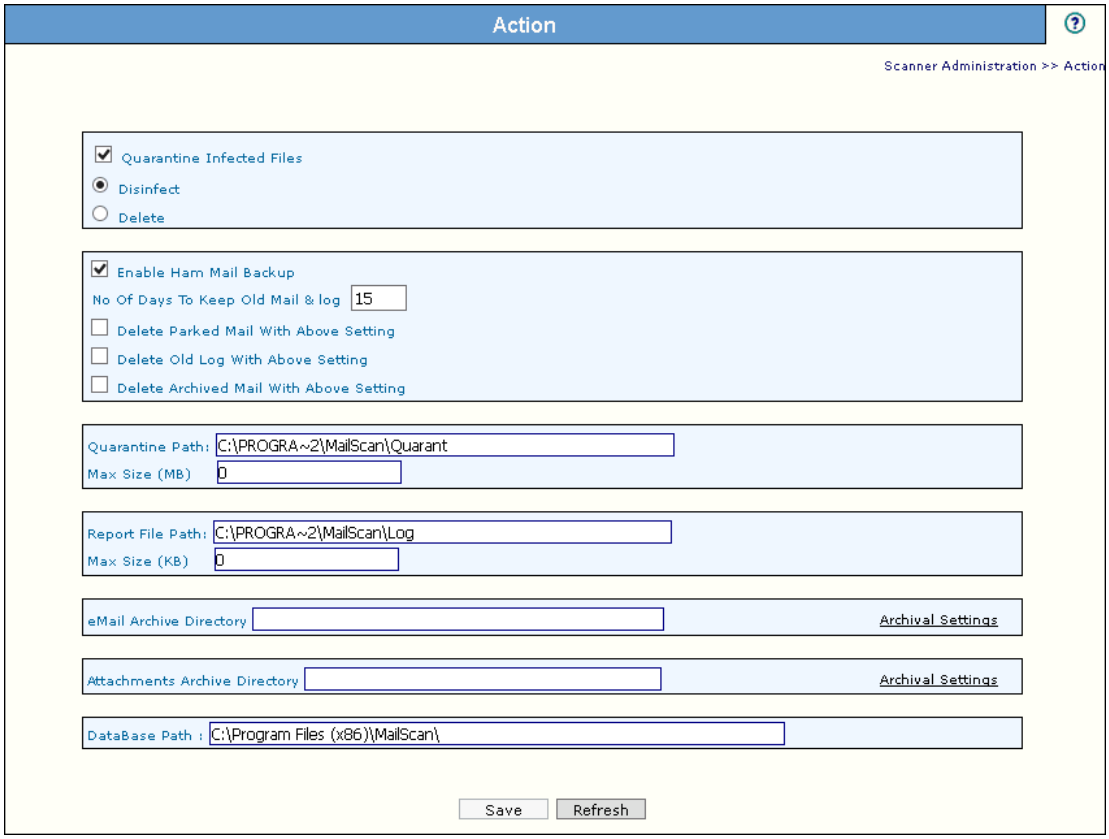
View Logs

MailScan maintains activity logs on daily basis; you can view these logs by clicking on Logs option. Logs are maintained in Log folder in the MailScan installation path. Click on respective **Date** links to get detailed views of the logs.



Configuring Logs

You can configure the Log option, by clicking **Change Path** link. **Action** window appears and configure following settings:



- Select the **Quarantine Infected Files** checkbox, to set actions that need to be performed on infected quarantine files. You can select below option:
    - **Disinfect**: This option will disinfect the infected quarantine files.
    - **Delete**: This option will directly delete the infected quarantine files.
- Select the **Enable Ham Mails Backup** checkbox, to create the backup of the Ham emails. Further, you can configure the following options:
    - No. Of Days To Keep Old Mails & log
    - Delete Parked Mail With Above Setting
    - Delete Old Log With Above Setting
    - Delete Archived Mail With Above Setting
- You can change the Quarantine Path and set the size limit (MB) for storing the quarantined emails. The default path is **C:\Program Files\MailScan\Quarant [32bit OS]** OR **C:\Program Files (x86)\MailScan\Quarant [64bit OS]**
- You can change the report file path and set the size limit (KB) for storing the logs files. The default path is **C:\Program Files\MailScan\Log [32bit OS]** OR **C:\Program Files (x86)\MailScan\Log [64bit OS]**
- You can configure the setting for archiving emails; you can enter the path for storing archived emails in **eMail Archive Directory** textbox. You can further configure the settings for archival settings by clicking on **Archival Settings** option present on the interface. Learn more about **Archival**, by clicking **here**.
- You can add path to store the archived attachments in **Attachments Archive Directory** textbox.
- You can change the **DataBase Path**. The default path is **C:\Program Files\MailScan\ [32bit OS]** OR **C:\Program Files (x86)\MailScan\ [64bit OS]**

Flush Logs

This page lets you delete log files generated by MailScan.

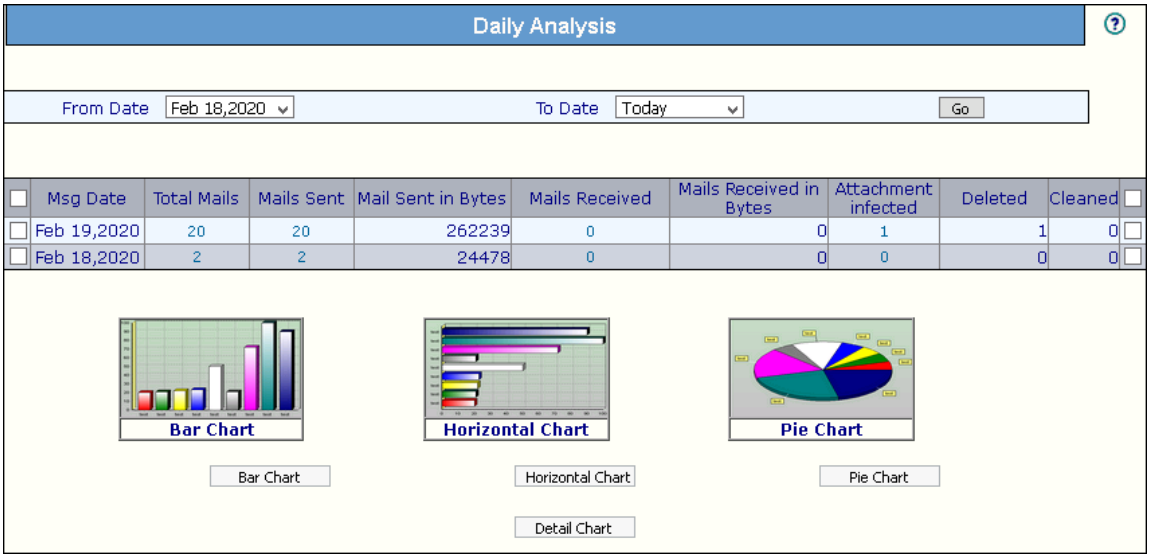
To delete all logs, click **Yes**.

Reports

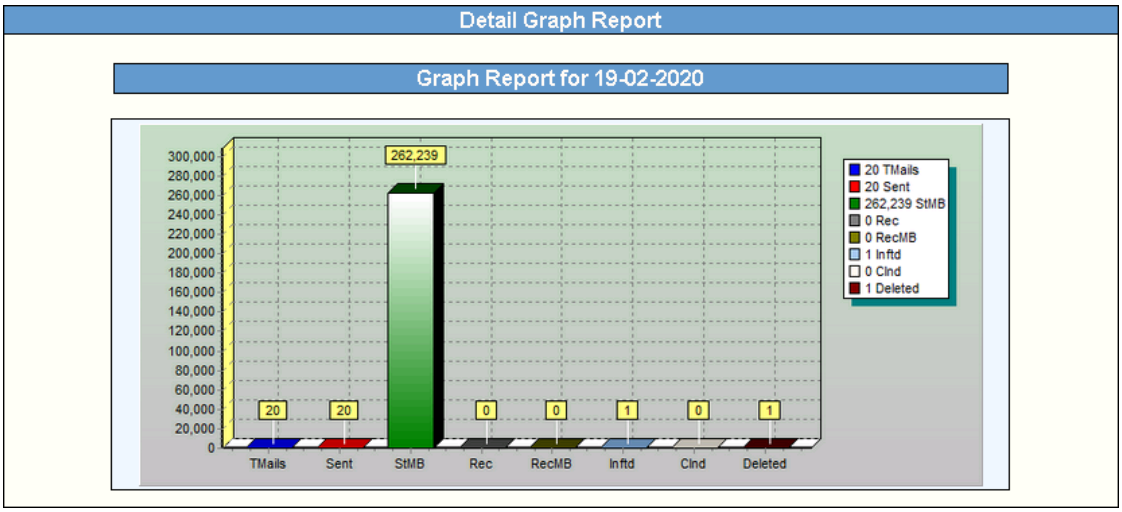
The Reports submodule provides a report of MailScan activity for a period. These pages provide reports about different MailScan tasks. The reports consists of total number of emails sent and received, email size (in bytes), infected attachments, deleted emails, cleaned emails and quarantined emails.

Reports

This setting provides a report of MailScan activity for a period. These pages provide reports about different MailScan tasks. This page will display the daily analysis of the reports for a specific period in a tabular and graphical format.

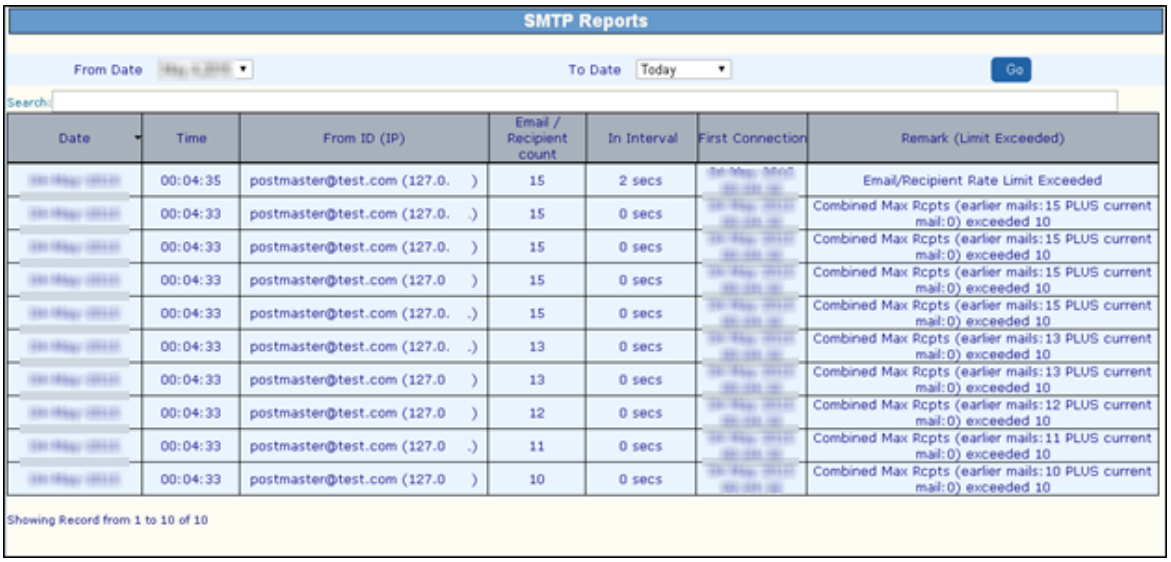


You can also get the detailed view of the chart by selecting particular time period and then clicking on **Detail Charts**.



SMTP Reports

It allows you to capture report for the packet transfer that takes place through your Mail Server.

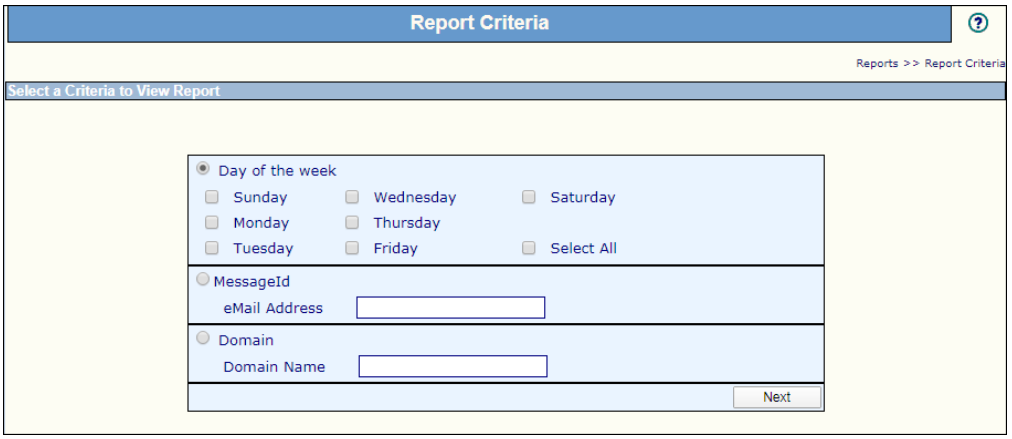


The report includes following data

- **From Date/To Date**: You can select the range of dates to be covered in the report.
- **Date**: Displays the date on which the email was sent.
- **Time**: Displays the time, email was sent.
- **From ID (IP)**: Displays the email address as well as IP address from which the email was sent.
- **Email / Recipient count**: Displays the number of recipient to which the email was sent.
- **In Interval**: Displays the time (in seconds) in which the emails were sent to the recipients.
- **First Connection**: Displays date and time when the mail server initiated sending the mails
- **Remark (Limit Exceeded)**: Displays a message in case message exceeds the number of recipients permitted.

Report Criteria

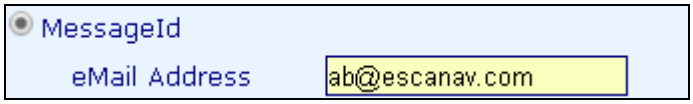
It allows you to define Criteria for generating MailScan Activity report. You can define the Day on which the report will be generated or you can select all days to generate report daily. It also allows you to specify email address to which the report will be sent automatically. Additionally, you can define the Domain for which the report will be generated or you can specifically define the email address that you want to monitor and generate report for a specific period of time.



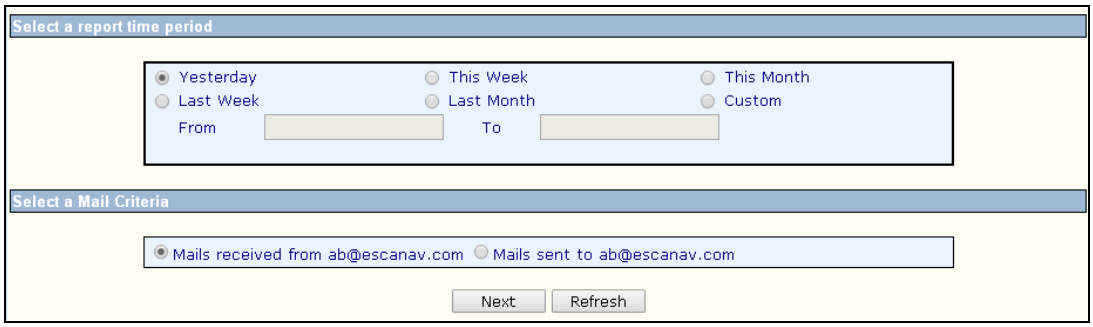
Generating a Report

To generate a report for specific for email address, follow the below steps:

1. Select the **MessageId** option and enter the email address that you wish to monitor or generate report for in the respective field for **eMail Address**.



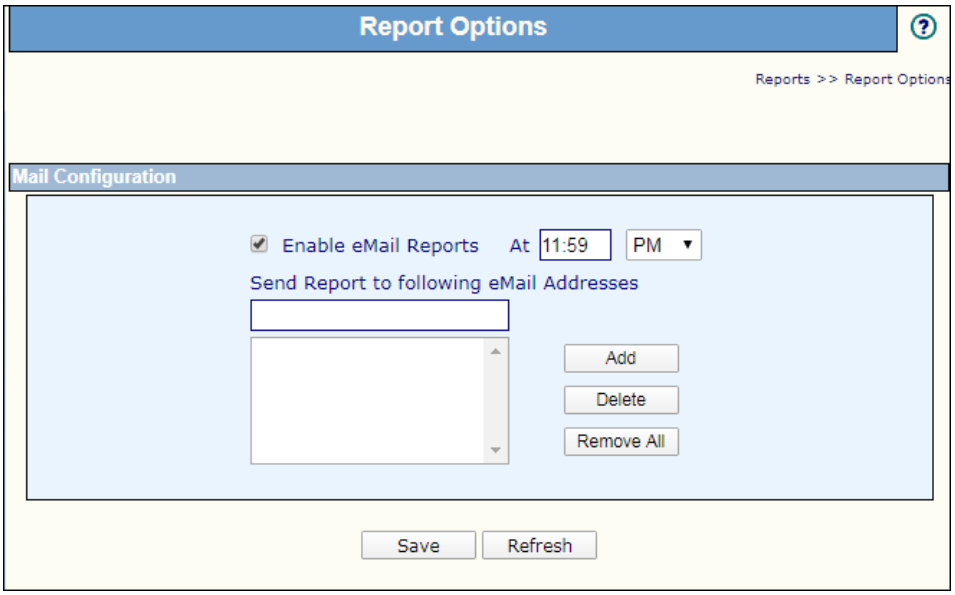
2. Click **Next**. Select the desired option for Report time period.
3. Now Select the desired option for Generating report for received email or sent by the specified email address.



4. Click **Next**, you will be forwarded to the following interface, it displays the report for the specified email address for the defined time period. Click on **Show Graph** option to view report in graphical format.

Report Options

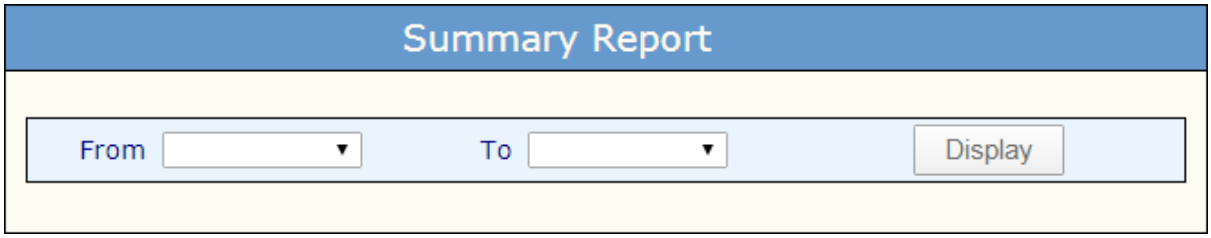
This page allows you to define settings for the time of the day at which the report should be generated. You can also define the email addresses to which the report will be sent automatically by MailScan.



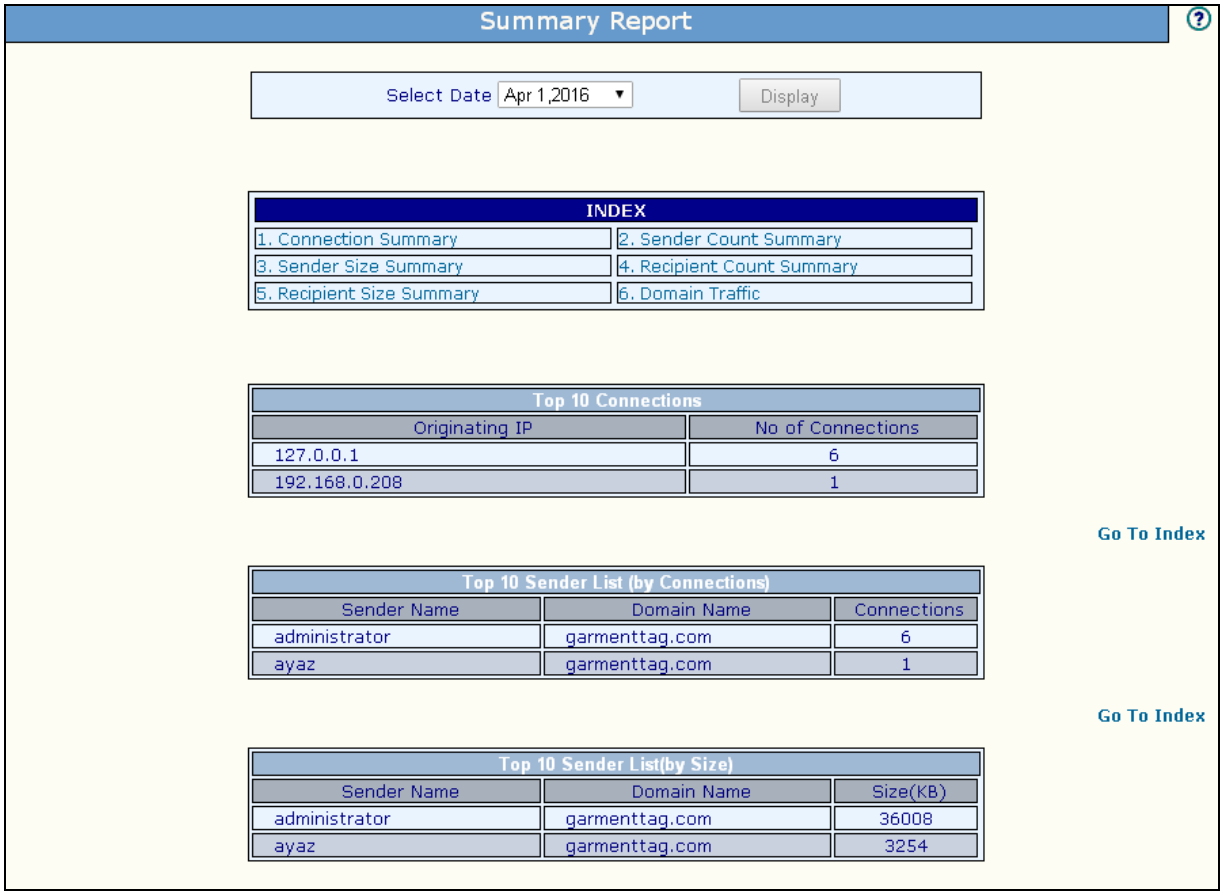
After you are done with the changes, click **Save**. Click **Refresh** to refresh the interface.

Summary Report

This option lets you view the summary report for MailScan for a given date.

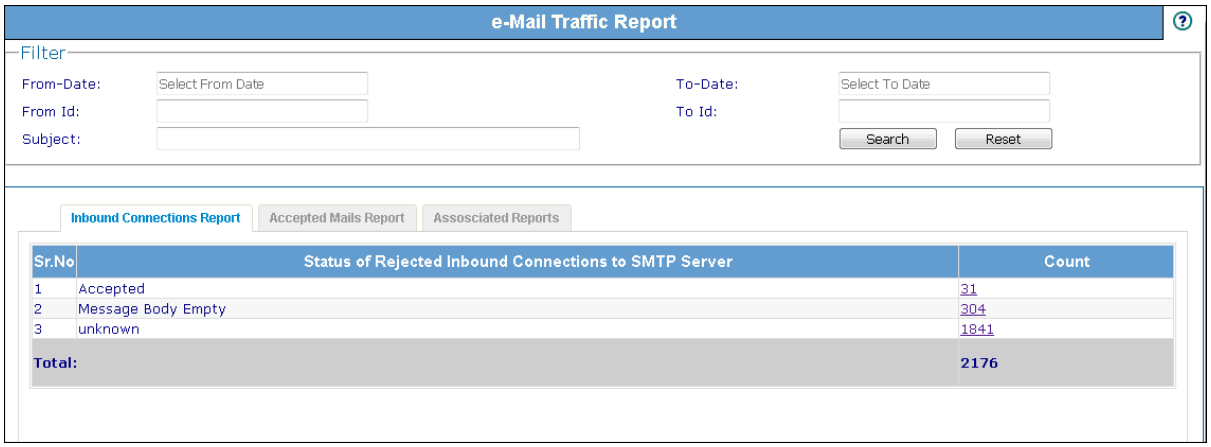


Click the dropdown for both **From** and **To** boxes and select the preferred duration, and then click **Display**.
The Summary Report appears.



Email Traffic Report

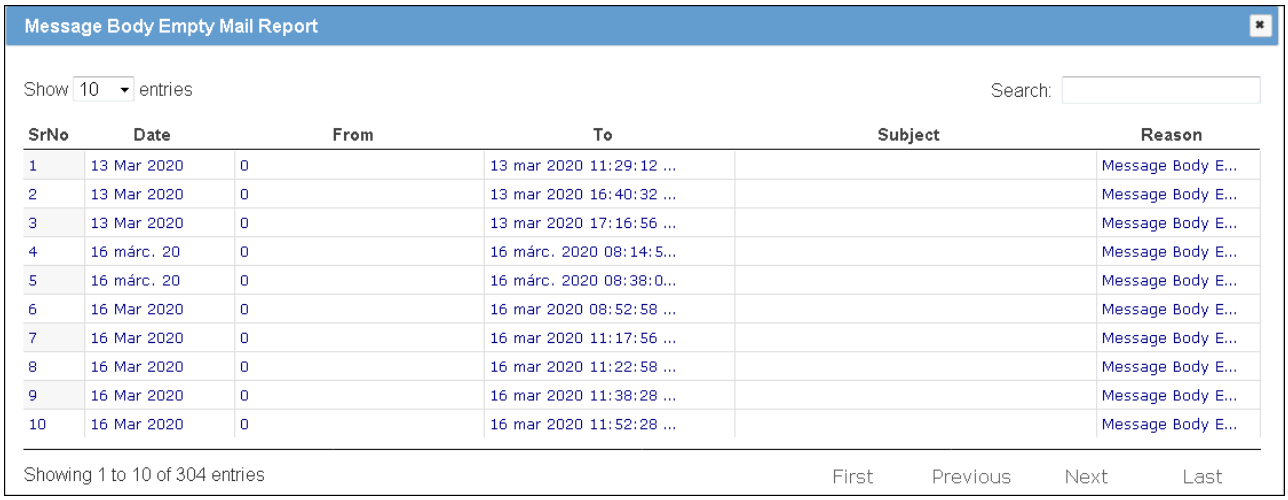
This page will provide the email traffic reports that offer a clear insight on the mailbox traffic by numbers. These reports provide a helpful resource for monitoring and reviewing mailbox flow, as well as helping Exchange managers keep a watchful eye on the organization's use of mailboxes. Administrators will also track everyday traffic along with the historic traffic.



You can filter out the reports based on the date, email IDs, and Subject. It has three tabs, which are as follows:

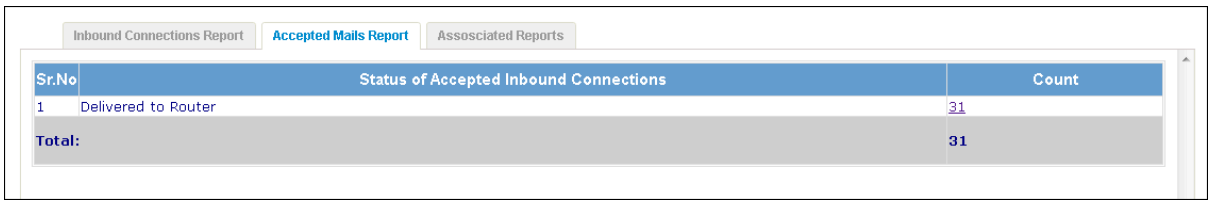
Inbound Connection Report

This tab will provide the real-time email status report of the inbound connections. Click on the count to get the detailed view of the report.



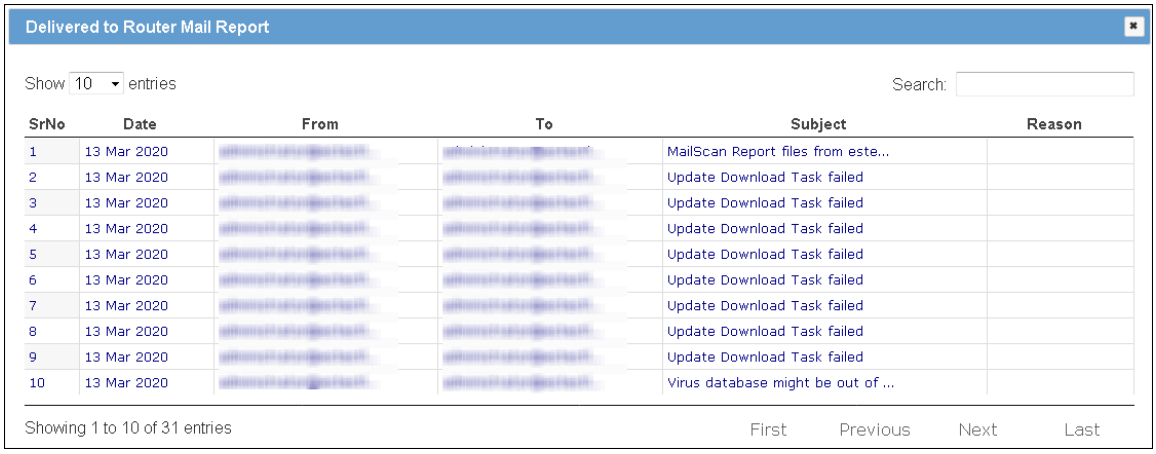
Accepted Mails Reports

This tab will provide the real-time email status report of the accepted emails.



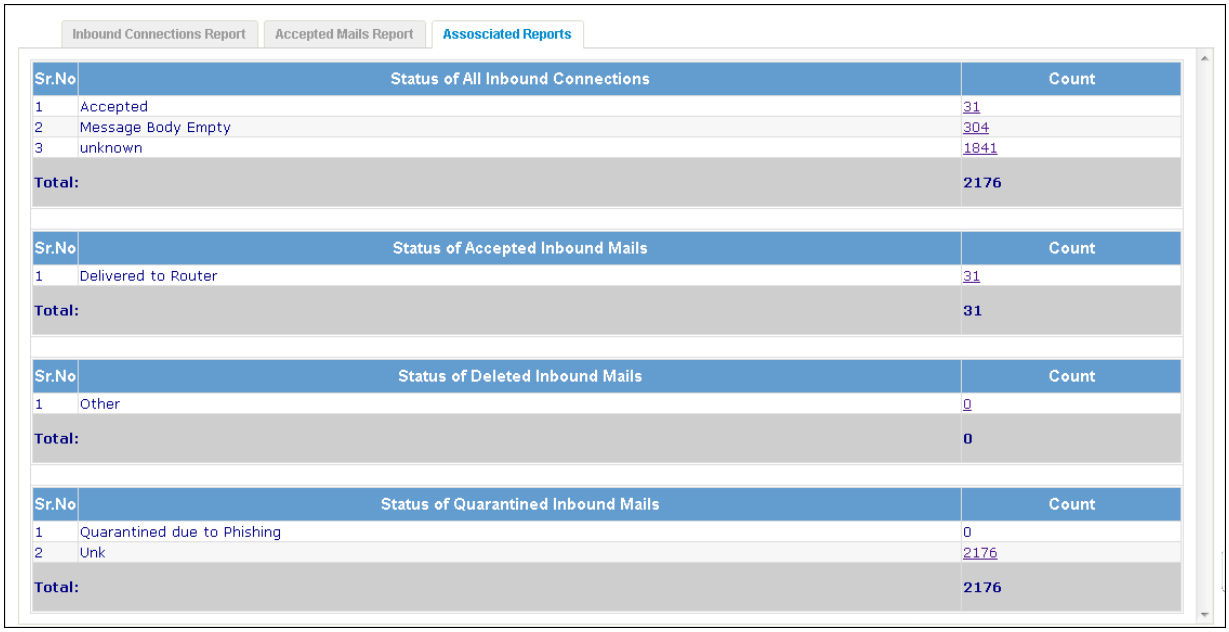
Sr.No	Status of Accepted Inbound Connections	Count
1	Delivered to Router	31
Total:		**31**

You can get the detailed view by click on the number in the **Count** column.



Associated Reports

This tab will provide the real-time email status report of the associated emails.



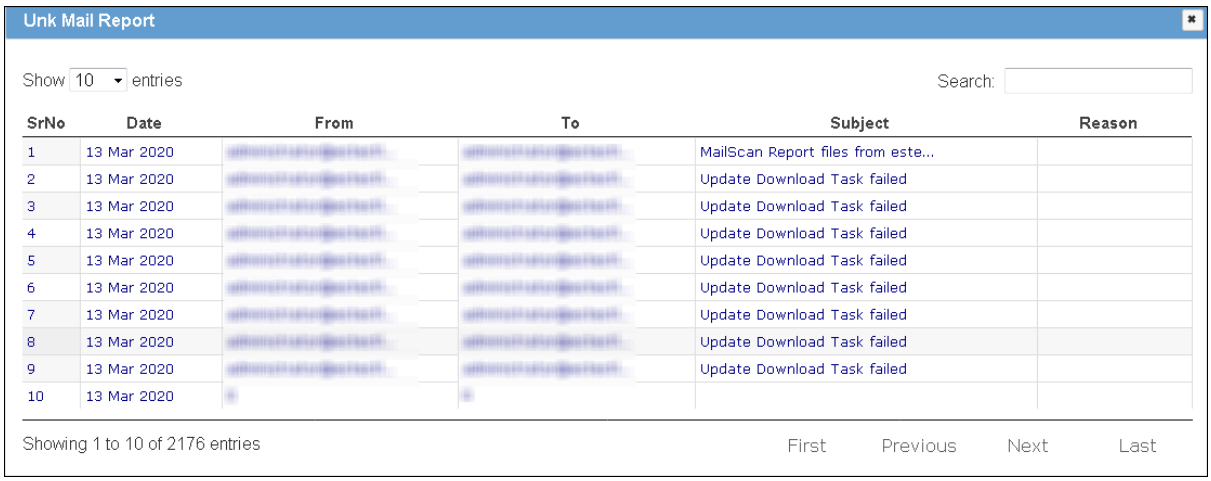
Sr.No	Status of All Inbound Connections	Count
1	Accepted	31
2	Message Body Empty	304
3	unknown	1841
Total:		**2176**

Sr.No	Status of Accepted Inbound Mails	Count
1	Delivered to Router	31
Total:		**31**

Sr.No	Status of Deleted Inbound Mails	Count
1	Other	0
Total:		**0**

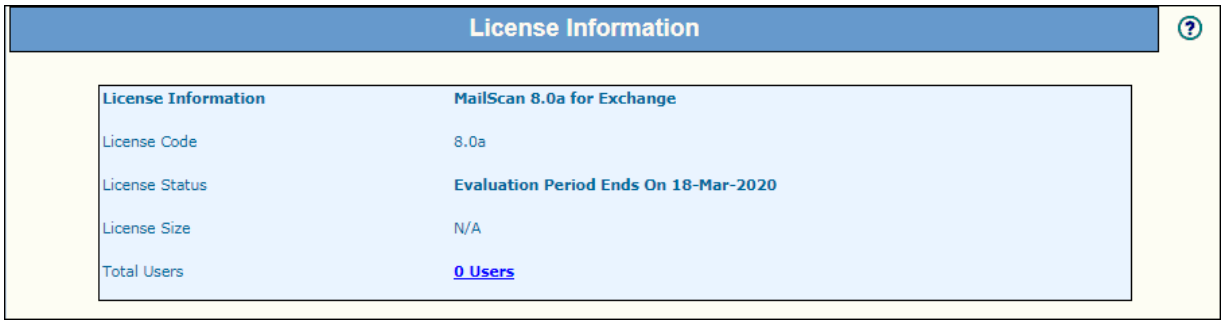
Sr.No	Status of Quarantined Inbound Mails	Count
1	Quarantined due to Phishing	0
2	Unk	2176
Total:		**2176**

You can get the detailed view by click on the number in the **Count** column.



License Information

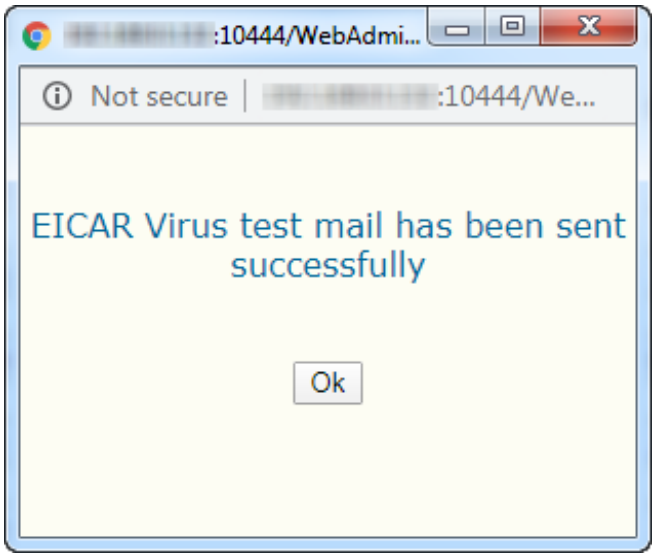
This page displays the license information for MailScan. The trial version is valid for 30 days. To run the MailScan beyond the trial period, purchase a license key by writing to us at sales@mwti.net.



Check RBL

MailScan for Exchange Servers connects to the URL www.whatismyipaddress.com site. This site provides IPs of known spammers and has active real time blacklists. You can verify any IP that connects to your mail server is listed and take the appropriate action.

Virus Test Mail



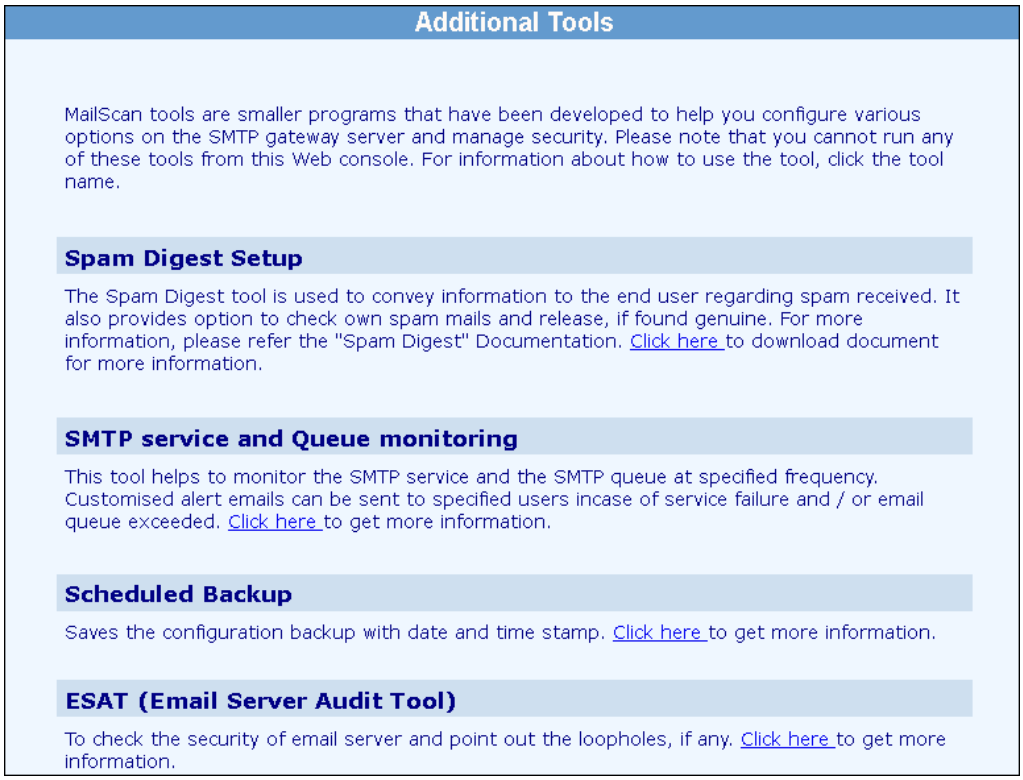
This feature lets you test MailScan for Anti-Virus effectiveness. An email is sent to the local domain, carrying a test virus. If you have configured the system correctly, the email is detected and actions you have specified like Quarantine, Delete, or Forward to Admin are run.

Help

This page will display the contact information for MicroWorld and view the information on each of the features of MailScan.

Additional Tools

MailScan tools are smaller programs that have been developed to help you configure various options on the SMTP gateway server and manage security. Please note that you cannot run any of these tools from this Web console. For information about how to use the tool, click the tool name.



This screen will has following tools and description to how to configure them:

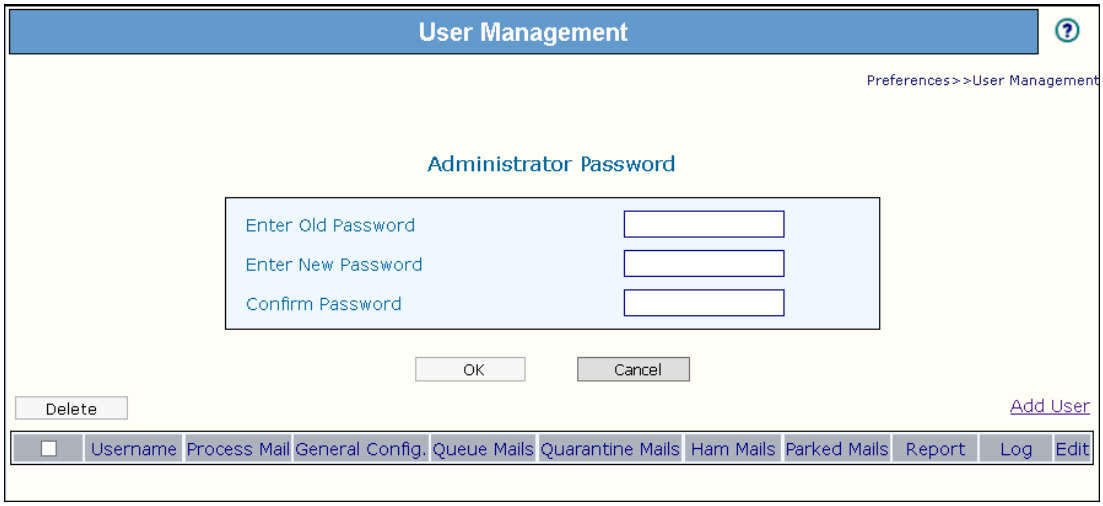
- Spam Digest Setup
- SMTP service and Queue monitoring
- Scheduled Backup
- ESAT (Email Server Audit Tool)

Preferences

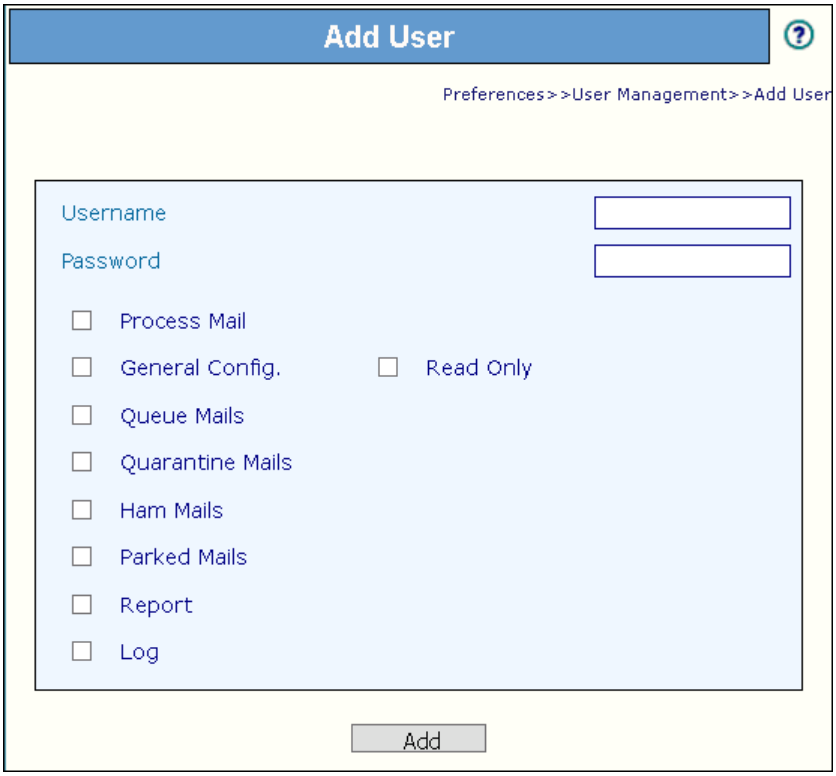
This section lets you configure the password and authentication settings.

User Management

This page lets you change the password or add users that can access MailScan.



You can add user by clicking on **Add User** link present in right-hand of the screen.



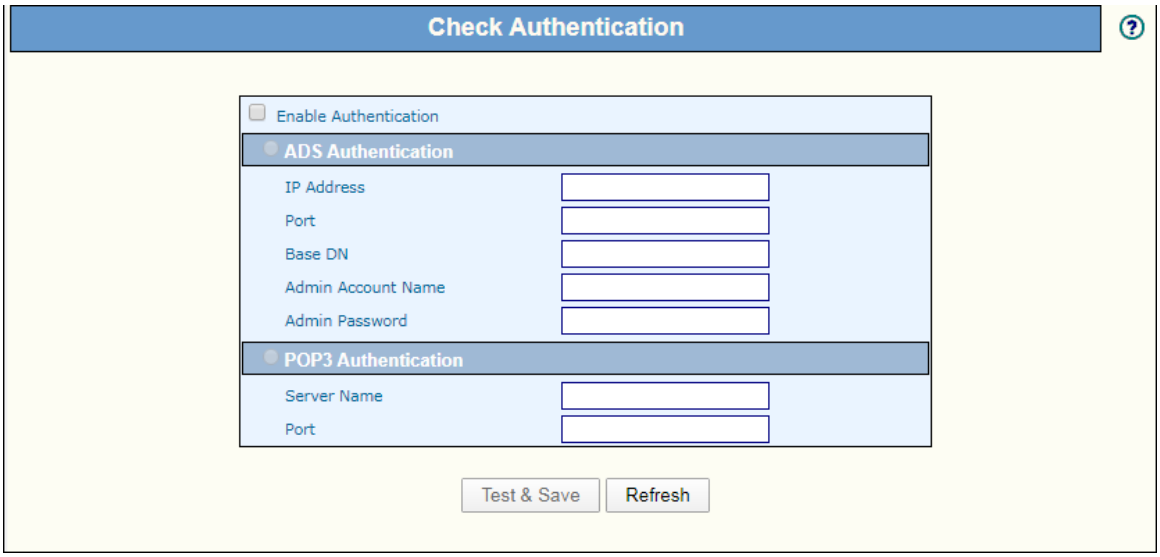
Add User window appears. Provide username and password for the user along with actions that user can take.

- Process Mail
- General Config.
- Queue Mails
- Quarantine Mails
- Ham Mails
- Parked Mails
- Reports
- Logs
- Read Only

After filling all the details, click **Add**.

Check Authentication

This submodule lets you configure ADS and POP3 authentication settings. Active Directory Service (ADS) is an implementation of LDAP directory services by Microsoft. The main purpose of Active Directory is to provide central authentication and authorization services for Windows-based computers. Active Directory also allows administrators to assign policies, deploy software, and apply critical updates to an entire organization.
Post Office Protocol 3 (POP3) is the most recent version of a standard protocol for receiving email. POP3 is a client/server protocol in which email is received and held for you by your Internet server. Periodically, you (or your client email receiver) check your mailbox on the server and download any email, probably using POP3. This standard protocol is built into most popular email products, such as Eudora and Outlook Express. It's also built into the Netscape and Microsoft Internet Explorer browsers.



- **Enable Authentication**: Click on the option to enable Authentication in MailScan Web admin. The authentication may be ADS authentication or POP3 authentication.
- **ADS Authentication**: This will allow users to check their own quarantined emails. The Active directory credentials are shared with the user. To configure this enter the IP Address where Active Directory Server is hosted and the port number for ADS Server. Enter Base DN value for AD Server and administrator Account Name; this user should be present on AD Server as well. Enter the Password for Admin.

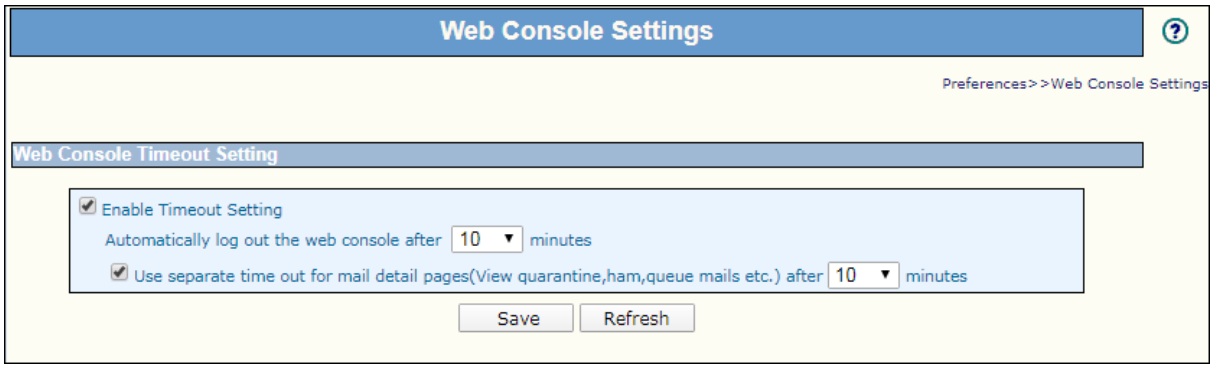
- **POP3 Authentication**: This will allow users to retrieve a quarantined email from the mail server. POP3 authentication will authenticate users connecting to the mail server. To configure this option enter the IP Address of POP3 Server and port number where POP3 Server will listen for emails.

After you are done with the changes, click **Test & Save**. Click **Refresh** to refresh the interface.

Note	It is recommended to re-login to confirm the above configuration.

Web Console Settings

This page lets you configure the web console timeout settings.

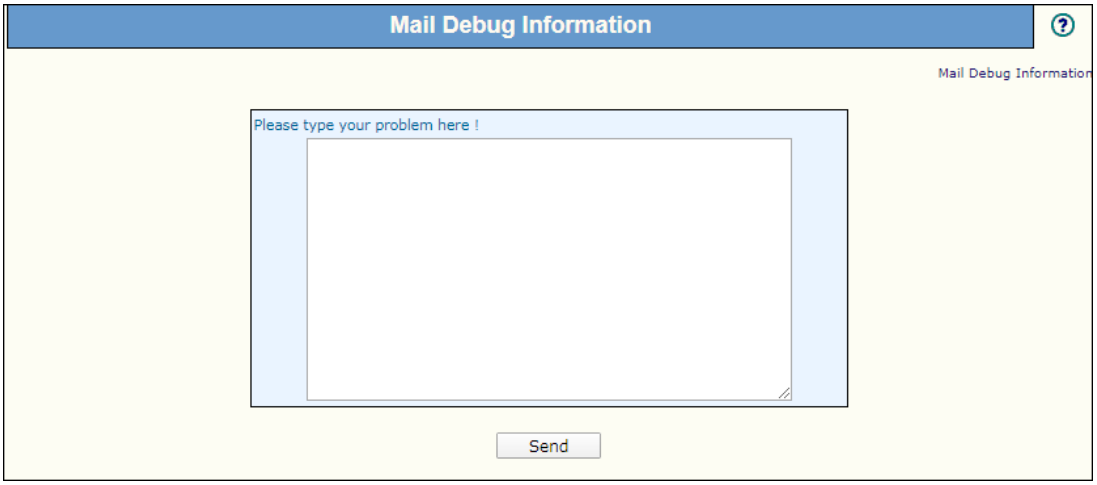


- **Enable Timeout Settings**: Select this option to enable timeout settings for MailScan Web administrator Module.
- **Automatically Logout the Web Console after __ Minutes**: Use this dropdown to define the time in minutes after which administrator will be logged out of MailScan if idle for the time period defined here.
- **Use time out for mail detail pages (view Quarantine, ham, queue mails etc.) after __ Minutes**: Use this drop down to define the time in minutes after which administrator will be logged out of mail detail pages (view quarantine, ham, queue mails, and more).

Enter the preferred duration and then click **Save**. Click **Refresh** to refresh the interface. The Web Console Settings gets saved.

Mail Debug Information

This section will allow you to email your MailScan-related problem (debug information) to the Administrator.



Enter your problem/query in the box and then click **Send**. The debug information that will be sent by MailScan is stored in **debugms.zip** in the **C:\Program Files (x86)\MailScan\Debug (64-bits)** or **C:\Program Files\MailScan\Debug (32 bits)** folder.