MySpamGuard 2.1
User Guide

Research & Development Unit
Open Source Competency Center (OSCC),
MAMPU,
Lot E302-34, Enterprise Building 3,
63000 Cyberjaya, Selangor
Tel: 03-83191200
Fax: 03-83193206

Table of Contents

Introduction

MySpamGuard is an email spam solution. It searches the headers and text of incoming emails to determine whether it is spam based on the procmail instruction or rules set by the user. MySpamGuard will classify the suspected spam accordingly; email sent by a virus, email from a known spam source which is definitely spam, and email which is probably spam. It then tags the filtered out email with the appropriate header and respond accordingly to the action specified by the users.

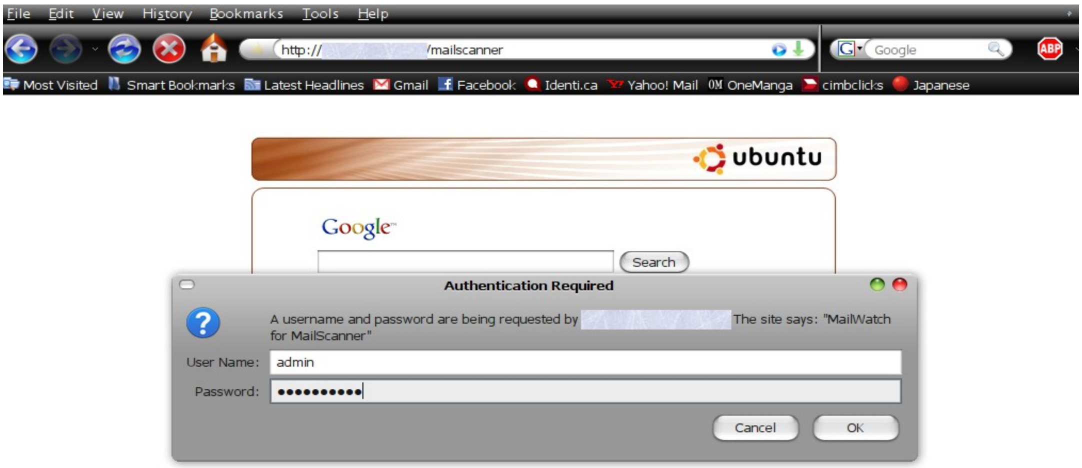
New features in MySpamGuard 2.1

- Easy installation process. The files needed will be downloaded automatically by the installer.
- All modules needed in MySpamGuard are combined as one package. The modules are:
  - SpamAssassin – spam checking aplication
  - MailScanner – email scanning for general filtering
  - ClamAV – anti virus solution
- Minimum configuration because most of the configuration is installed automatically by the installer
- Automatic update for all package from OSCC repository server

Login to MySpamGuard

Open url to login to the MySpamGuard. It will prompt for username and password. Then click on the OK button. Example as below:

> *Mail URL: http://DOMAIN_NAME/mailscanner*
>
> *Username: admin*
>
> *Password: admin (encrypted)*



http://[redacted]/mailscanner

Authentication Required

A username and password are being requested by [redacted] The site says: "MailWatch for MailScanner"

User Name: admin

Password: •••••••••••

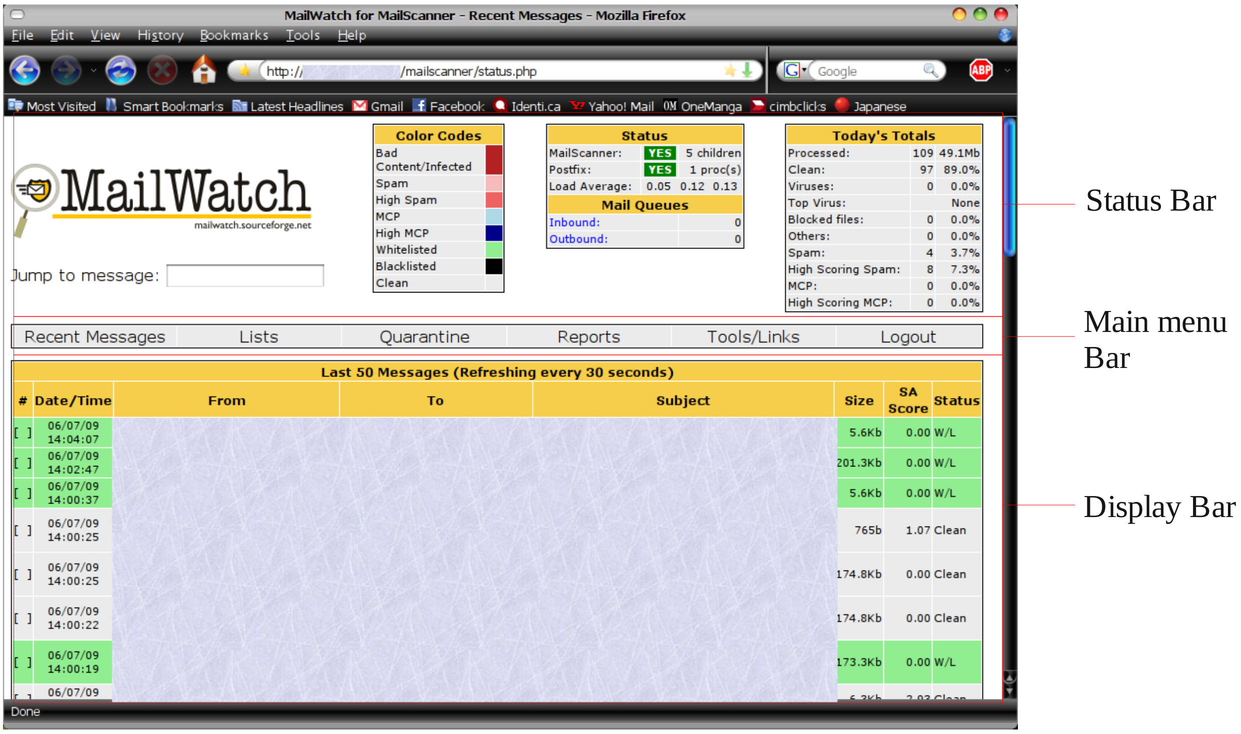
Figure 1

MailScanner are using MailWatch as front-end for user to check for process happened in the system.

MySpamGuard Dashboard

Right after you login to MySpamGuard, it will open up main page of MySpamGuard or also know as MySpamGuard Dashboard as shown in Figure 2. MySpamGuard Dashboard are divide into three section:

1. Status Bar
2. Main Menu Bar
3. Display Bar – Display for Main Menu Bar



Color Codes	
Bad Content/Infected	🟥
Spam	🟥
High Spam	🟥
MCP	🟦
High MCP	🟦
Whitelisted	🟩
Blacklisted	⬛
Clean	⬜

Status		
MailScanner:	YES	5 children
Postfix:	YES	1 proc(s)
Load Average:	0.05 0.12	0.13

Mail Queues	
Inbound:	0
Outbound:	0

Today's Totals		
Processed:	109	49.1Mb
Clean:	97	89.0%
Viruses:	0	0.0%
Top Virus:		None
Blocked files:	0	0.0%
Others:	0	0.0%
Spam:	4	3.7%
High Scoring Spam:	8	7.3%
MCP:	0	0.0%
High Scoring MCP:	0	0.0%

Last 50 Messages (Refreshing every 30 seconds)

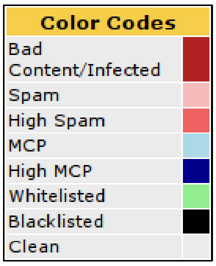
#	Date/Time	From	To	Subject	Size	SA Score	Status
[ ]	06/07/09 14:04:07	[redacted]	[redacted]	[redacted]	5.6Kb	0.00	W/L
[ ]	06/07/09 14:02:47	[redacted]	[redacted]	[redacted]	201.3Kb	0.00	W/L
[ ]	06/07/09 14:00:37	[redacted]	[redacted]	[redacted]	5.6Kb	0.00	W/L
[ ]	06/07/09 14:00:25	[redacted]	[redacted]	[redacted]	765b	1.07	Clean
[ ]	06/07/09 14:00:25	[redacted]	[redacted]	[redacted]	174.8Kb	0.00	Clean
[ ]	06/07/09 14:00:22	[redacted]	[redacted]	[redacted]	174.8Kb	0.00	Clean
[ ]	06/07/09 14:00:19	[redacted]	[redacted]	[redacted]	173.3Kb	0.00	W/L
[ ]	06/07/09	[redacted]	[redacted]	[redacted]	6.3Kb	2.03	Clean

Figure 2

Status Bar

MySpamGuard will display summary of process happened within system in Status Bar:

1. Color Codes



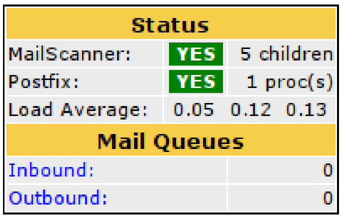
Color Codes	
Bad Content/Infected	🟥
Spam	🟥
High Spam	🟥
MCP	🟦
High MCP	🟦
Whitelisted	🟩
Blacklisted	⬛
Clean	⬜

Figure 3

Color Codes will differentiate incoming email into its category as shown in Figure 3.

For example: In Figure 2, we can identified incoming email that are listed under **Whitelisted** lists based from the color codes of that email.

2. Status and Mail Queues



Status			
MailScanner:	YES	5 children	
Postfix:	YES	1 proc(s)	
Load Average:	0.05	0.12	0.13

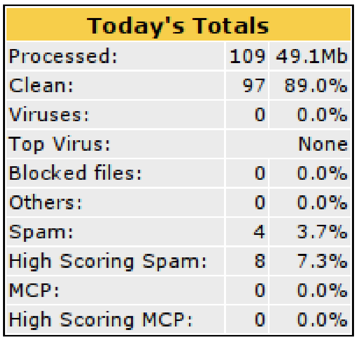
Mail Queues	
Inbound:	0
Outbound:	0

Figure 4

The status of main process that run the whole system will be shown in **Status** box.

As for **Mail Queues** is the total incoming or outgoing email that has been delayed.

3. Today's Totals



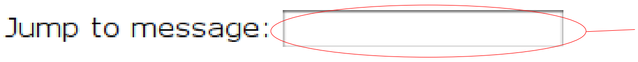
Today's Totals		
Processed:	109	49.1Mb
Clean:	97	89.0%
Viruses:	0	0.0%
Top Virus:		None
Blocked files:	0	0.0%
Others:	0	0.0%
Spam:	4	3.7%
High Scoring Spam:	8	7.3%
MCP:	0	0.0%
High Scoring MCP:	0	0.0%

Figure 5

From **Today's Totals** box, it will show you summary of today statistic.

4. Jump to message

Jump to message is an application for user to locate/view email summary by type in email ID in the field provide as shown in Figure 6



Insert Email ID in this field

Figure 6

Main Menu Bar and Display Bar

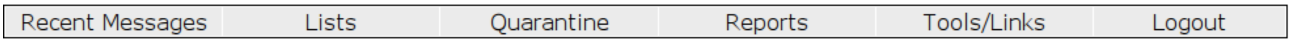


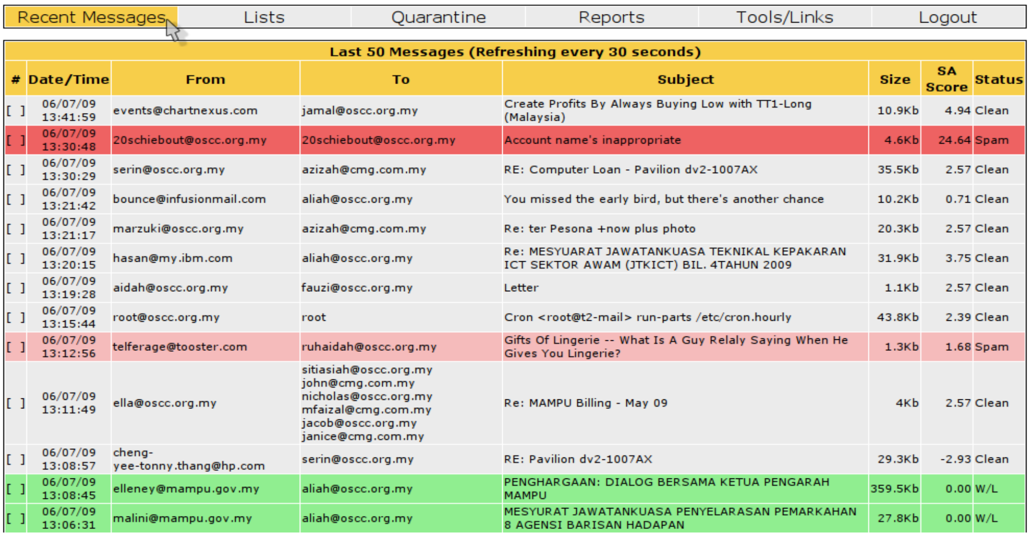
Figure 7

There are five (5) services can be choose from Main Menu Bar; the services choose will be shown in Display Bar:

1. Recent Messages
2. Lists
3. Quarantine
4. Reports
5. Tools/Links

Recent Messages

They will navigate to 50 latests messages, and it will refresh for every 30 seconds to update the latest list.

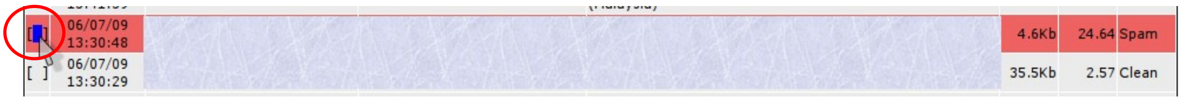


Last 50 Messages (Refreshing every 30 seconds)

#	Date/Time	From	To	Subject	Size	SA Score	Status
[ ]	06/07/09 13:41:59	events@chartnexus.com	jamal@oscc.org.my	Create Profits By Always Buying Low with TT1-Long (Malaysia)	10.9Kb	4.94	Clean
[ ]	06/07/09 13:30:48	20schiebout@oscc.org.my	20schiebout@oscc.org.my	Account name's inappropriate	4.6Kb	24.64	Spam
[ ]	06/07/09 13:30:29	serin@oscc.org.my	azizah@cmg.com.my	RE: Computer Loan - Pavilion dv2-1007AX	35.5Kb	2.57	Clean
[ ]	06/07/09 13:21:42	bounce@infusionmail.com	aliah@oscc.org.my	You missed the early bird, but there's another chance	10.2Kb	0.71	Clean
[ ]	06/07/09 13:21:17	marzuki@oscc.org.my	azizah@cmg.com.my	Re: ter Pesona +now plus photo	20.3Kb	2.57	Clean
[ ]	06/07/09 13:20:15	hasan@my.ibm.com	aliah@oscc.org.my	Re: MESYUARAT JAWATANKUASA TEKNIKAL KEPAKARAN ICT SEKTOR AWAM (JTKICT) BIL. 4TAHUN 2009	31.9Kb	3.75	Clean
[ ]	06/07/09 13:19:28	aidah@oscc.org.my	fauzi@oscc.org.my	Letter	1.1Kb	2.57	Clean
[ ]	06/07/09 13:15:44	root@oscc.org.my	root	Cron <root@t2-mail> run-parts /etc/cron.hourly	43.8Kb	2.39	Clean
[ ]	06/07/09 13:12:56	telferage@tooster.com	ruhaidah@oscc.org.my	Gifts Of Lingerie -- What Is A Guy Relaly Saying When He Gives You Lingerie?	1.3Kb	1.68	Spam
[ ]	06/07/09 13:11:49	ella@oscc.org.my	sitiasiah@oscc.org.my john@cmg.com.my nicholas@oscc.org.my mfaizal@cmg.com.my jacob@oscc.org.my janice@cmg.com.my	Re: MAMPU Billing - May 09	4Kb	2.57	Clean
[ ]	06/07/09 13:08:57	cheng-yee-tonny.thang@hp.com	serin@oscc.org.my	RE: Pavilion dv2-1007AX	29.3Kb	-2.93	Clean
[ ]	06/07/09 13:08:45	elleney@mampu.gov.my	aliah@oscc.org.my	PENGHARGAAN: DIALOG BERSAMA KETUA PENGARAH MAMPU	359.5Kb	0.00	W/L
[ ]	06/07/09 13:06:31	malini@mampu.gov.my	aliah@oscc.org.my	MESYURAT JAWATANKUASA PENYELARASAN PEMARKAHAN 8 AGENSI BARISAN HADAPAN	27.8Kb	0.00	W/L

Figure 8

User can also review email summary by checking the # box, as shown in Figure 9.

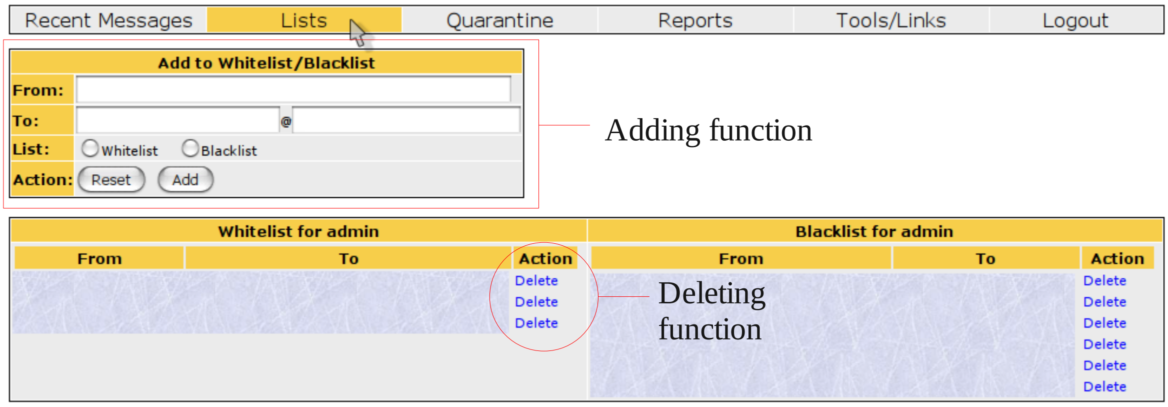


[■]	06/07/09 13:30:48	4.6Kb	24.64	Spam
[ ]	06/07/09 13:30:29	35.5Kb	2.57	Clean

Figure 9

Lists

Using **Lists** service, user can manually add new Whitelist/Blacklist address into the system.



Add to Whitelist/Blacklist

From:

To: @

List: ○ Whitelist ○ Blacklist

Action: Reset Add

Adding function

Whitelist for admin		
From	To	Action
		Delete
		Delete
		Delete

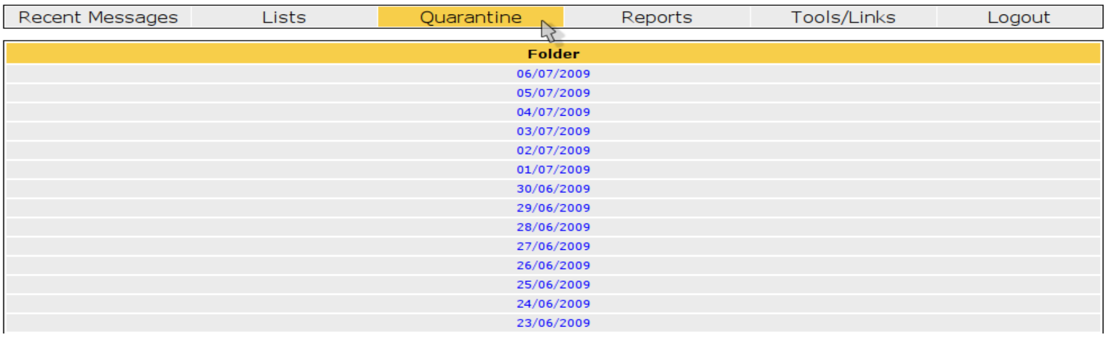
Blacklist for admin		
From	To	Action
		Delete
		Delete
		Delete
		Delete
		Delete
		Delete

Deleting function

Figure 10

1. Adding new address into Lists
   - Fill in the field in the **Add to Whitelist/Blacklist** Box with the sender and recipient address.
   - Next, check either radiobutton **Whitelist** or **Blacklist**.
   - Finally, click button **Add** to update the new address.
2. Deleting address from Lists
   - Click **Delete** from the **Action** column in the **Whitelist for admin** or **Blacklist for admin**

Quarantine

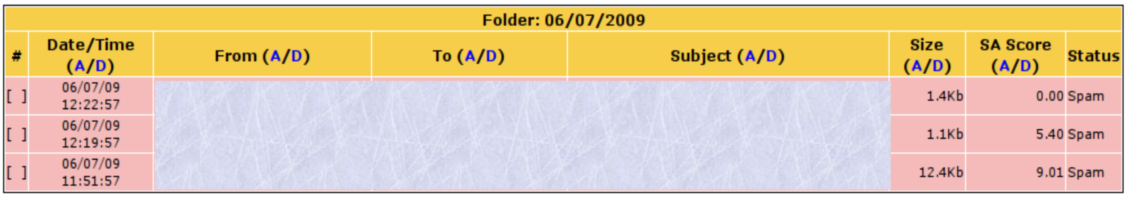


Recent Messages	Lists	Quarantine	Reports	Tools/Links	Logout

Folder
06/07/2009
05/07/2009
04/07/2009
03/07/2009
02/07/2009
01/07/2009
30/06/2009
29/06/2009
28/06/2009
27/06/2009
26/06/2009
25/06/2009
24/06/2009
23/06/2009

Figure 11

All email that is calculated with lower spamassassin (SA) score, will be stored in Quarantine. Email with lower SA score will be stored by their respective date. Example as shown in Figure 12 and Figure 13.

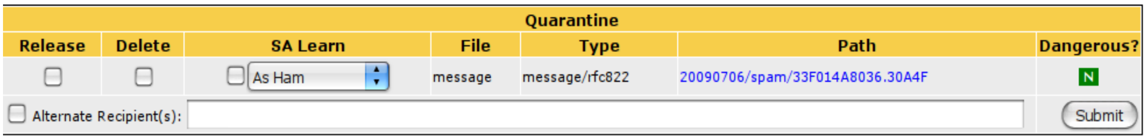


Folder: 06/07/2009

#	Date/Time (A/D)	From (A/D)	To (A/D)	Subject (A/D)	Size (A/D)	SA Score (A/D)	Status
[ ]	06/07/09 12:22:57	[redacted]	[redacted]	[redacted]	1.4Kb	0.00	Spam
[ ]	06/07/09 12:19:57	[redacted]	[redacted]	[redacted]	1.1Kb	5.40	Spam
[ ]	06/07/09 11:51:57	[redacted]	[redacted]	[redacted]	12.4Kb	9.01	Spam

Figure 12

Click on directory to view email listing on that respective date. Click on # column in order to view email summary. Scroll to the end of the email summary to view Quarantine box.



Quarantine

Release	Delete	SA Learn	File	Type	Path	Dangerous?
□	□	□ As Ham	message	message/rfc822	20090706/spam/33F014A8036.30A4F	N
□ Alternate Recipient(s):						Submit

Figure 13

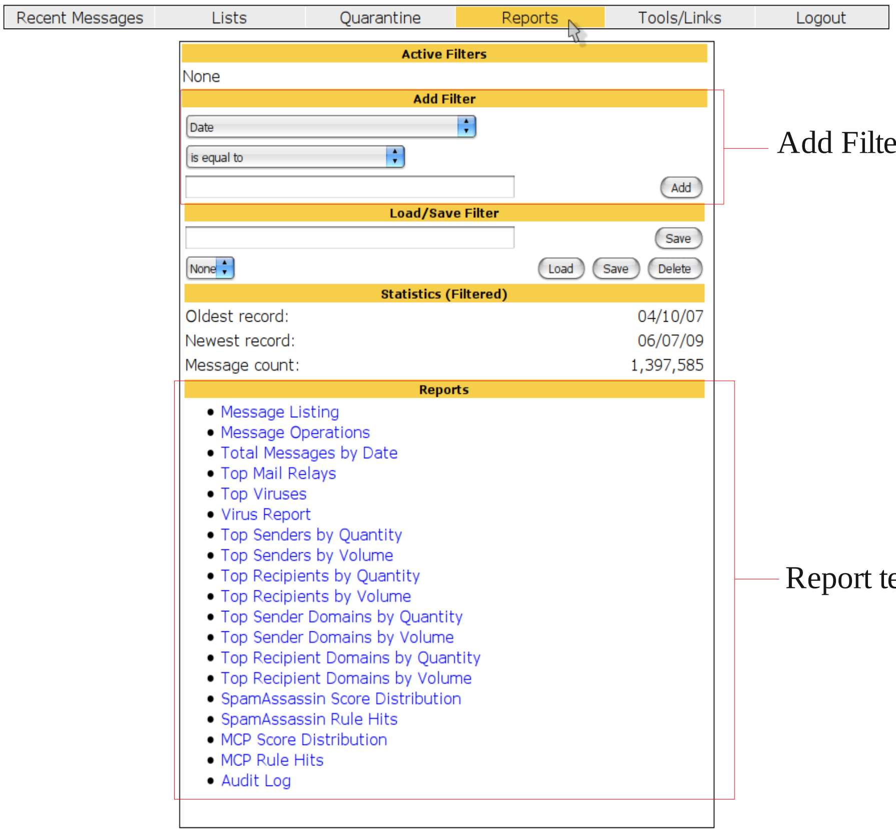
There are few options available in Quarantine box, such as:

- Release or Delete options
- SA Learn : An enhancement for system to recognize email pattern, be it spam or ham(clean) email.

Reports

Service to generate report based from few options available in the **Reports** section, as shown in Figure 14. User can also change variable for the report by adding new filter in the **Add Filter** section.

In **Statistic (Filtered)** section will list out statistic of incoming email in your system from oldest record to newest record define in your Active Filter



Active Filters

None

Add Filter

Date

is equal to

Load/Save Filter

None

Statistics (Filtered)

Oldest record:	04/10/07
Newest record:	06/07/09
Message count:	1,397,585

Reports

- Message Listing
- Message Operations
- Total Messages by Date
- Top Mail Relays
- Top Viruses
- Virus Report
- Top Senders by Quantity
- Top Senders by Volume
- Top Recipients by Quantity
- Top Recipients by Volume
- Top Sender Domains by Quantity
- Top Sender Domains by Volume
- Top Recipient Domains by Quantity
- Top Recipient Domains by Volume
- SpamAssassin Score Distribution
- SpamAssassin Rule Hits
- MCP Score Distribution
- MCP Rule Hits
- Audit Log

Add Filter section

Report template

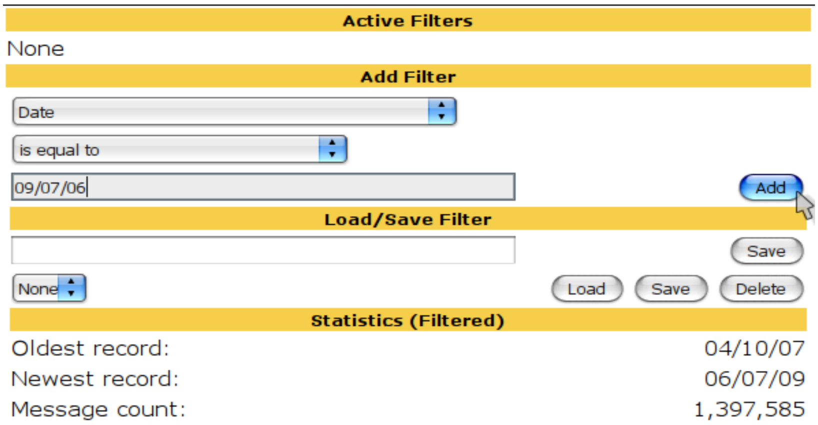
Figure 14

1. Adding filter

   - Example: Change period (date) to generate report.
   - First, in the **Add Filter** section, choose variable to use in the Filter. Since we are going to change period use in the system, choose **Date** from the drop down menu.
   - Next, change the variable for the **Date** from the drop down menu to **is equal**

to.

- Then, key in date as in format YY/MM/DD as shown in the Figure 15.



Active Filters

None

Add Filter

Date

is equal to

09/07/06

Load/Save Filter

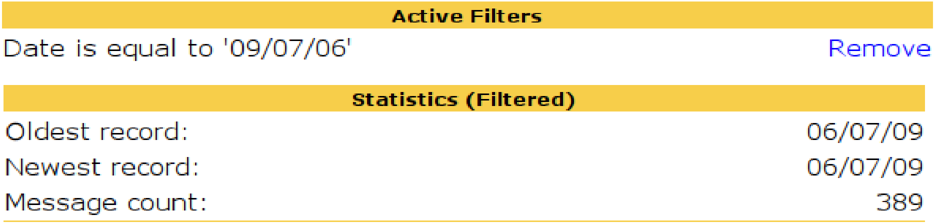
None

Statistics (Filtered)

Oldest record:	04/10/07
Newest record:	06/07/09
Message count:	1,397,585

Figure 15

- Finally, click button **Add** to submit new filter in the system. As shown in Figure 16, It has update **Active Filters** to **Date is equal to '09/07/06'**. Total count email for the 06 July 2009 is 389 number of emails.



Active Filters

Date is equal to '09/07/06'

Statistics (Filtered)

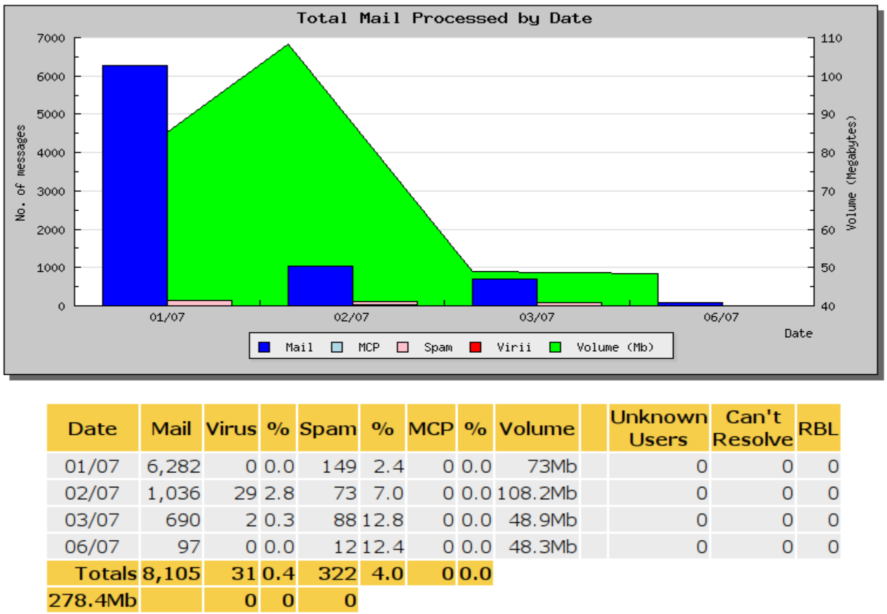
Oldest record:	06/07/09
Newest record:	06/07/09
Message count:	389

Figure 16

3. Selecting report template from Reports listing

- First, you have to add new variable in the **Add Filter** section as in previous example.

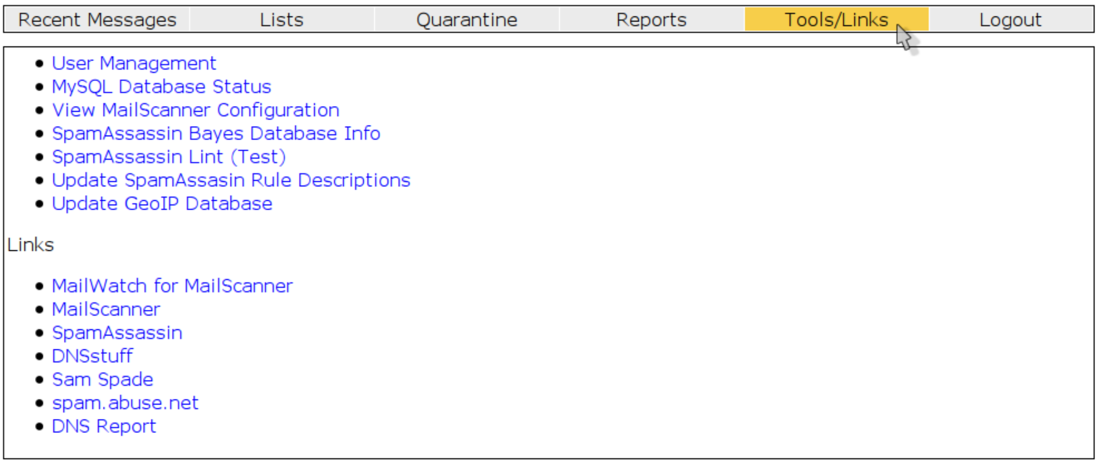
- Next, choose one of options available in the **Reports** section. Example of report on **Total Mail Processed by Date** from **01 July 2009 until 06 July 2009**



Date	Mail	Virus	%	Spam	%	MCP	%	Volume		Unknown Users	Can't Resolve	RBL
01/07	6,282	0	0.0	149	2.4	0	0.0	73Mb		0	0	0
02/07	1,036	29	2.8	73	7.0	0	0.0	108.2Mb		0	0	0
03/07	690	2	0.3	88	12.8	0	0.0	48.9Mb		0	0	0
06/07	97	0	0.0	12	12.4	0	0.0	48.3Mb		0	0	0
Totals	**8,105**	**31**	**0.4**	**322**	**4.0**	**0**	**0.0**					
278.4Mb		**0**	**0**	**0**								

Figure 17

Tools/Links



- User Management
- MySQL Database Status
- View MailScanner Configuration
- SpamAssassin Bayes Database Info
- SpamAssassin Lint (Test)
- Update SpamAssasin Rule Descriptions
- Update GeoIP Database

Links

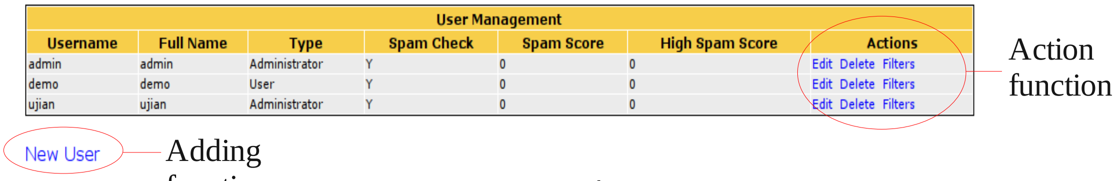
- MailWatch for MailScanner
- MailScanner
- SpamAssassin
- DNSstuff
- Sam Spade
- spam.abuse.net
- DNS Report

Figure 18

Tools/Links provide service such as:

1. User management

   - Administrator can add new user to the system, delete or edit existing user in the system
   - First, click on **User Management** from the list available.
   - It will display **User Management** box. Administrator have options to apply action available in the **Actions** column for existing user.



User Management

Username	Full Name	Type	Spam Check	Spam Score	High Spam Score	Actions
admin	admin	Administrator	Y	0	0	Edit Delete Filters
demo	demo	User	Y	0	0	Edit Delete Filters
ujian	ujian	Administrator	Y	0	0	Edit Delete Filters

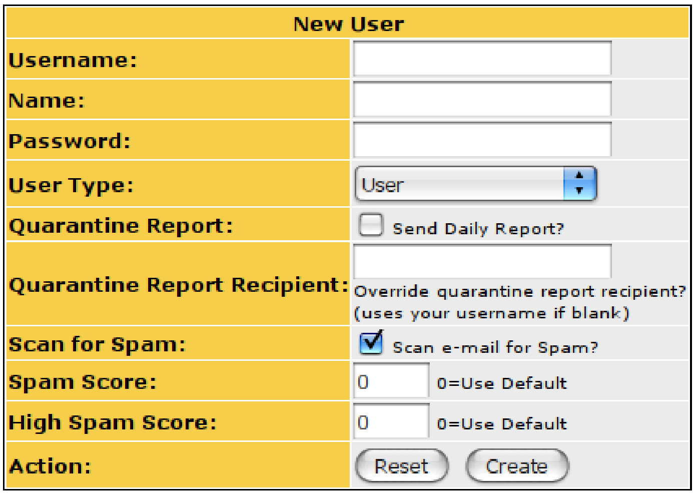
New User

Action function

Adding function

Figure 19

   - Aside from that, administrator also have the options to add new user into the system by click **New User** underneath **User Management** box. Click **New User** to display **New User** box as shown in Figure 20.



New User

Username:	
Name:	
Password:	
User Type:	User
Quarantine Report:	□ Send Daily Report?
Quarantine Report Recipient:	Override quarantine report recipient? (uses your username if blank)
Scan for Spam:	☑ Scan e-mail for Spam?
Spam Score:	0 0=Use Default
High Spam Score:	0 0=Use Default
Action:	Reset Create

Figure 20

   - Fill in the requirement field in order to add new user into the system.
   - Once you finish fill in all the requirement field, click button **Create** to submit new user in the system.

2. Update status for MySQL by click link **MySQL Database Status**.
3. Viewing configuration MailScanner to check on spamassassin score and other configuration by click link **View MailScanner Configuration**.
4. Updating Spamassassin rules in the system by click link **Update SpamAssassin Rule Description**.

Maintenance

The following should be checked on a regular basis:

Network connections

The administrator should verify the server is reachable from the public network to avoid service interruption. Network monitoring is beyond the scope of these manual.

Log files

With the log files, it is possible to identify and monitor hardware and software problems on the servers. The log files should be checked at least once a week. All log files in /var/log/ directory.

Services

Used to start, stop or cancel a service on a local or remote computer. It is also a tool to set up recovery actions to take place if a service should fail. Should be checked in case of service failure.

e.g:

```
#/etc/init.d/[service_name] start/stop/status
```

Package update/patch

Check that the latest package update/patches has been installed on the servers. It should be checked and done at least once a month.

Disk Space

to verify that there is always enough space on the most mission critical servers. It should be done at least once a week. Use *df -lh* command.

Password change

Password should be changed periodically, at least every three months.

ClamAV update

Execute command *freshclam* frequently to verify automatic update is successfully done.

Check SpamAssassin rules

Execute command *sa-update -D* at least once a month to download the latest spamassassin rules.