Business Grade Email Security

Spam, Virus and Email Content Management

Administrators Reference Manual

Revision 4.0 – October 2004
Pacific Internet: business.techsupport@pacific.net.au
Ph: 13 36 39
Web: www.pacific.net.au

Table of Contents

#

1 Introduction

Welcome to CleanMail and thank-you for subscribing to our service. As an organisation and a dedicated team of people – we look forward to adding value to your business, and working with you into the future.

Pacific Internet is a leading Australian business Internet Communications Service Provider (ICSP) committed to delivering value and high quality solutions to customers.

We part of Pacific Internet Limited (NASDAQ: PCNTF), the largest telco-independent ICSP in the Asia Pacific region by geographic reach, with operations in Australia, Singapore, Hong Kong, the Philippines, India, Thailand and Malaysia, servicing over 472,000 customers.

We welcome your input and thoughts about our service – so if you have any questions about this user manual, the service – or about email content filtering, viruses, spam or privacy issues – please don't hesitate to contact us by emailing us at feedback@pacific.net.au
#

1.1 What is CleanMail?

CleanMail — Anti-Spam, Anti-Virus & Content Filtering

CleanMail is a fully managed anti-spam, anti-virus and content filtering email management solution *(powered by McAfee, Sophos Anti-Virus and Guardian – CleanMail's own heuristic technology)* that diligently protects organisations from viruses and unwanted emails without the need to purchase any software or hardware.

Today, with more than 36% of businesses believing that staff spend more than 30 minutes a day dealing with SPAM[1], and over 95% of viruses being transmitted by email[2] - CleanMail provides an easy to implement solution that shows an immediate, visible and ongoing benefit, whilst remaining extremely cost-effective for business.

CleanMail provides detailed information and control over the types and sizes of email attachments that are sent and received by an organisation's users.

Key statistics such as email sent and received by person, types of attachments and average size allows the company to better manage Internet bandwidth. Rules set to manage content and keywords allow organisations to control, monitor and limit legal exposure due to inappropriate or offensive email content.

##
[1] NSW Government Study, April 2004
[2] Ferris Research

1.2 How CleanMail benefits you

- **PEACE OF MIND –** You are able to focus on building and managing your business, with the confidence that CleanMail is on the job - constantly monitoring, updating and managing your email spam, virus & content security whilst protecting against potential attacks on your business systems;

- **SAVE TIME & MONEY -** As CleanMail stops junk mail, viruses and unwanted emails before they arrive at your network; this results in a substantial reduction in the amount of email traffic your servers need to contend with. This translates to real financial savings in server upgrades, management, and bandwidth fees.

- **EASE (& SAVINGS) OF INSTALLATION -** nothing to install (no hardware or software required), simple to manage (management is optional), simple to protect - within 48 hours of completing an application, CleanMail is protecting your business and systems.

- **BUSINESS SECURITY –** CleanMail provides the best available, industry leading email anti-virus and anti-spam protection that effectively stops email borne threats at the Internet – before they are able to enter your network, systems and subsequently compromise confidentiality/reliability of your files, data and systems.

- **ACCESS TO EXPERT RESOURCES –** CleanMail empowers your business with the expertise of a dedicated team of email security specialists focused on protecting your business from email based threats;

- **FLEXIBILE –** Although CleanMail is fully managed, we also provide you with a sophisticated web management console that facilitates access to usage statistics and management over your policies 24 x 7.

- **PROTECTING YOUR NETWORK –** CleanMail provides a clean stream of email to your mail servers/firewall, protecting your network from overload and outage caused by email denial of service, dictionary attacks, spam and viruses.

1.3 Key Features

- **EFFECTIVE & EASY TO MANAGE EMAIL ANTI-SPAM –** Stops SPAM and junk mail entering your business at the Internet – before it reaches your network. SpamGuard®, CleanMail's anti-spam service provides a hybrid best of breed solution for effectively stopping spam, whilst also providing extensive management tools to make spam management a simple task for your business;

- **BLANKET EMAIL ANTI-VIRUS -** Stops all viruses before they enter your network, and stops viruses from being sent to your clients & suppliers;

- **ATTACHMENT FILTER -** Controls the delivery of attachments by type – i.e. Stop **Movie files, music files, photos** etc by individual user or everyone;

- **STOP/CONTROL LARGE ATTACHMENTS -** Managed per email address or globally, CleanMail stops large attachments at the ISP before they are sent to your network;

- **TAILORED EMAIL FOOTERS -** automatically add company disclaimers or promotional information to every outgoing email;

- **OFFENSIVE LANGUAGE FILTERING** – CleanMail may be configured to quarantine, alert or warn of inappropriate or offensive language use in your company email.

- **CONFIDENTIAL FILE FILTERING** – Control distribution of confidential documents - and stop them leaving the office via email;

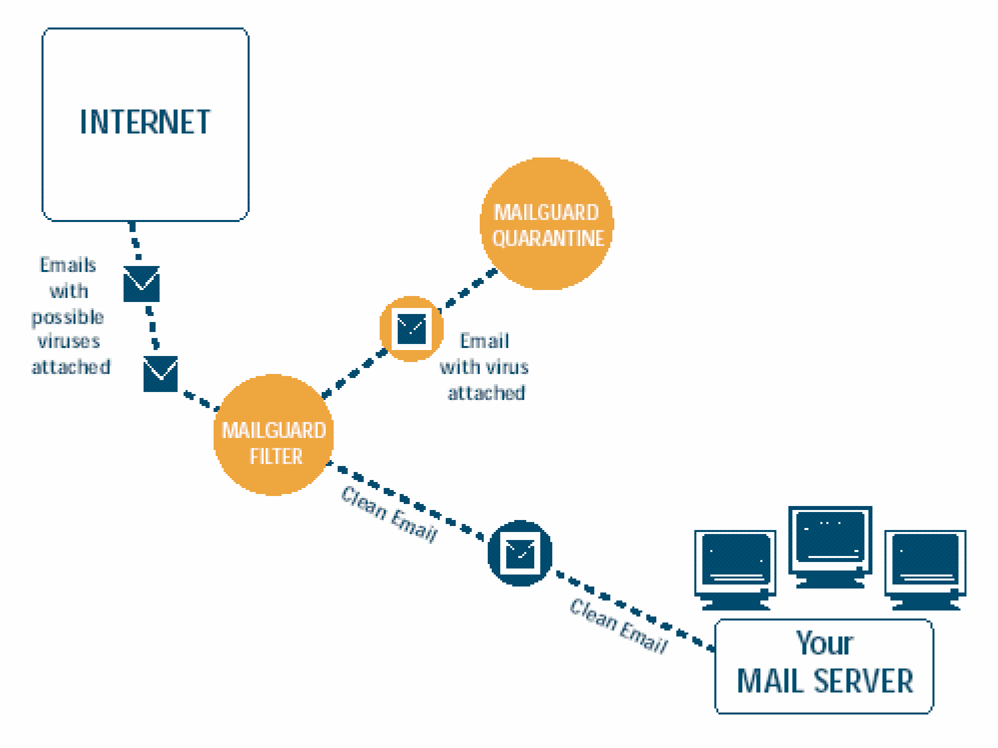
- **AUSTRALIAN PRIVACY ACT 2000 Compliant** – CleanMail provides the required tools to facilitate compliance with the email requirements of the Privacy Act 2000, in force as of December 21st, 2001;

- **INFORMATION & STATISTICS -** CleanMail provides comprehensive email statistics.

#

1.4 *How Does CleanMail Work?*

CleanMail works by intercepting every email that is sent to and from your Internet domain *(eg. yourdomain.com.au).* CleanMail then applies the policies that you have set for Anti-Spam, Anti-Virus and content filtering, and elects to take specified actions – or allow the email through to your mail server, for delivery to your desktop.



1.4.1 CleanMail Fully Fault Tolerant

#

The CleanMail service operates over dedicated servers distributed over many secure data hosting sites throughout Australia and overseas *(at time of writing 9 sites in Australia, and 3 in the US)*. These servers operate at different locations, and are connected to high bandwidth Internet connections to various Internet service providers.

When someone sends email to your organisation – it may be received by ANY of the CleanMail servers, and processed for anti-spam, anti-virus and content filtering. All of our servers are in “full synchronization” 24 hours of the day, and perform instant replication of all logs, policies and changes that may occur throughout our network.

Hence, the end result is that even if one, or two ISPs become unavailable, or one of our data centres goes off the air – as a client, your email, both incoming and outgoing, remains unaffected.

#

1.4.2 World Leading Anti-Virus Technology (Sophos & McAfee)

The front-line of CleanMail's anti-virus technology is provided by the combined resources of two of the world's leading anti-virus technology companies; Sophos & McAfee.

CleanMail engineers maintain regular communications with the virus labs of our anti-virus partners. We work collaboratively to assist in making them aware of suspicious files that are potentially viral that we've come across. We also receive regular security briefings directly from the global heads of these organisations.

CleanMail virus signatures are automatically updated every 10 minutes, compared to once a day or hour for most desktop/network based anti-virus solutions.

CleanMail's support level with Sophos & McAfee is that of a partner representing tens of thousands of people, which we translate to the best available email anti-virus protection for your business.

SOPHOS
SOPHOS ANTI-VIRUS

MAILGUARD®
GUARDIAN

McAfee®
SECURITY

1.4.3 CleanMail Guardian – Powerful Heuristic Technology

CleanMail utilises both the Sophos and the McAfee anti-virus engines as our first line of defence against all known viruses. However, often when a virus is first released "into the wild" it has not yet been identified and classified by the anti-virus vendors.

This window of time between when a virus is released, and when your desktop anti-virus is updated and will protect you from these viruses is usually measured in hours and often days.

During this window – CleanMail's Guardian engine uses sophisticated heuristics and statistical analysis of the millions of emails that transit our network every day to continue providing protection for your business.

By analysing patterns of messages and quarantining emails that contain potentially malicious, but as yet unidentified viruses – we are then able to work collaboratively with our anti-virus partners to effectively provide the best available protection for our clients against both known and unknown viruses.

#

#

#

1.5 CleanMail – Helping protect your network

1.5.1 Secure Mail Relay

Once CleanMail has been configured for your email domain, it becomes the “visible” email and domain addresses for communicating to your business.

When a person is attempting to unlawfully access your network, their first step is to try to access your business over the Internet. The first thing that they will attempt to find is your “IP address” – i.e. 203.36.42.1. This IP address is the public address of your network, and can be likened to a street address.

When the “would be” intruder performs a DNS lookup of your IP address (or primary MX record), it is similar to them looking up your address in a whitepages directory. Once they have your address, it makes it easier for the visitor to then come to your house and start testing your local security…

With CleanMail in place, when the visitor performs a lookup for your address, they are pointed towards CleanMail. Your address is kept private. Not unlike a Post Office Box or silent phone number.

The CleanMail servers have been systematically strengthened to stop visitors from attempting to get past our servers. They perform a function similar to a steel security door that sits in front of your “normal entry door”, keeping visitors from attempting to break in – or in reality hack at your mail servers’ vulnerabilities.

1.5.2 Redundancy & security

Normally, email over the Internet is sent from mail server to mail server. If for some reason your mail server is not available on the Internet for any period of time – it may be possible that an embarrassing message is sent back to the sender “cannot contact this organisation – have given up”. This type of message implies a lack of professionalism in your organisation’s ability to manage their email.

With CleanMail in place, CleanMail’s redundant server network acts to receive the email and then try on a regular basis to communicate with your mail server.

CleanMail’s servers are located at high bandwidth co-location centres that provide us with 24 x 7, backup power and generator access. In the unlikely case that one of our data centres becomes unavailable for any reason, all mail is automatically routed through our other data centres.

2 How to setup CleanMail

After you have completed your initial application form for CleanMail, and sent the ***"MX Change Request"*** fax to your Internet provider, CleanMail will begin filtering your inbound email over the next 48-hour period[3].

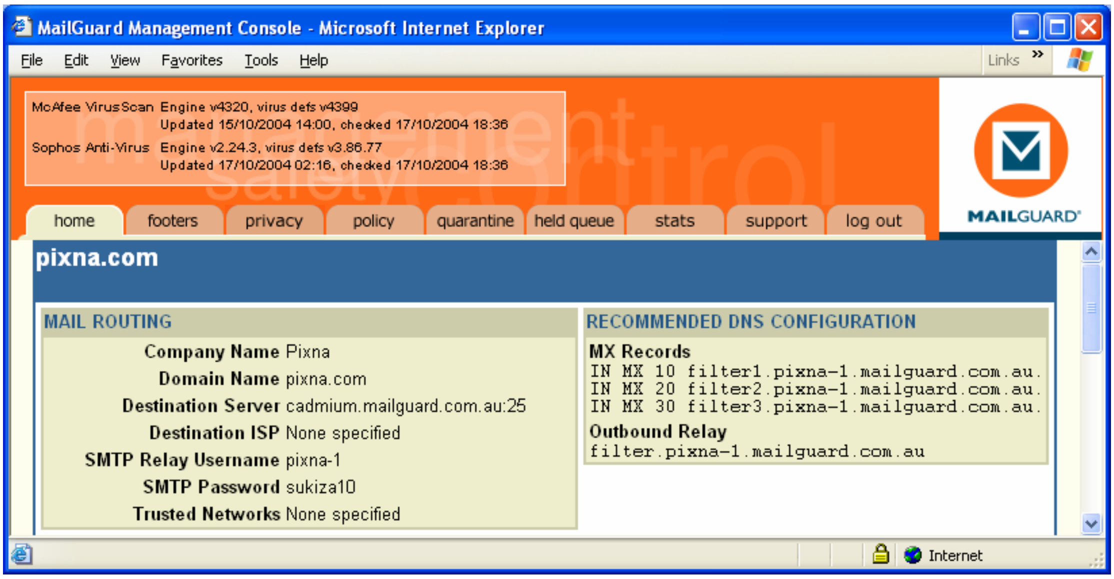
After this initial 48-hour period, all of your incoming email will be pre-filtered by CleanMail with our default protection policy.

2.1 Outgoing Email

In order to begin filtering outgoing email, you must set your mail server, or individual email clients (if you do not have a mail server) to send all of their outgoing email via to:

filter.xxxxxx-x**.CleanMail.com.au**

The exact address for this is specified in your welcome email documentation, and is also accessible from your CleanMail Management console by selecting the View button next to the selected domain from the **home** tab, as shown below.



McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 18:36
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 18:36

pixna.com

MAIL ROUTING

Company Name	Pixna
Domain Name	pixna.com
Destination Server	cadmium.mailguard.com.au:25
Destination ISP	None specified
SMTP Relay Username	pixna-1
SMTP Password	sukiza10
Trusted Networks	None specified

RECOMMENDED DNS CONFIGURATION

MX Records

```
IN MX 10 filter1.pixna-1.mailguard.com.au.
IN MX 20 filter2.pixna-1.mailguard.com.au.
IN MX 30 filter3.pixna-1.mailguard.com.au.
```

Outbound Relay

```
filter.pixna-1.mailguard.com.au
```

All of your settings for incoming, and outgoing email are available from this screen.

Once this has been configured, all of your outgoing email will be automatically filtered via the CleanMail service.

For further details on configuring your specific Mail Server please consult the websites listed in your welcome email or contact your IT manager / IT consultant.

##

[6]#F r qvhuydwlyh#ÈWlp h#wr#OlyhŠ#hvwlp dwh1#Xvxdo| #wklv#ghod| #z rxog#udqj h#ehwz hhq#4#kr xu#dqg#57#kr xuv1#

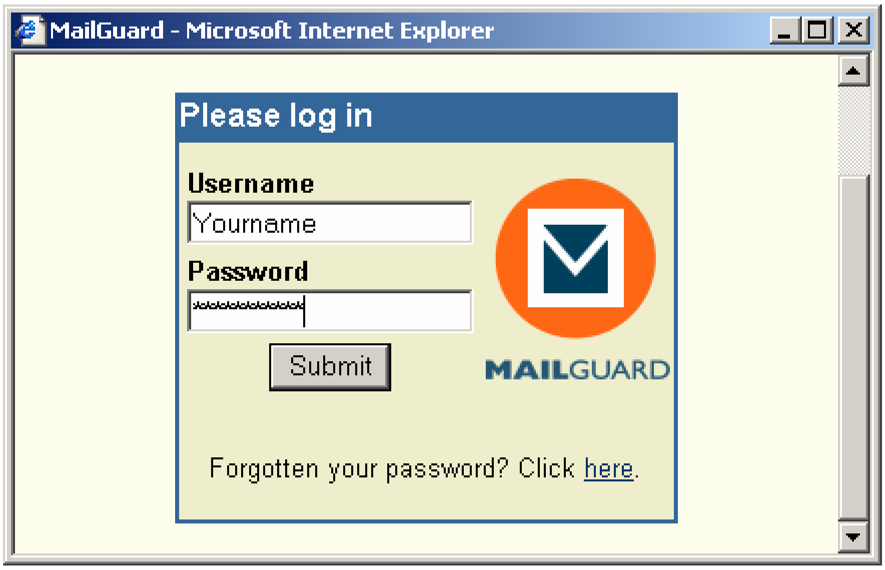
#

3 Navigating the CleanMail Management Console

3.1 *Logging in – https://login.mailguard.com.au*

#

3.2 The CleanMail service is managed through a secure browser interface to the management console. This can be reached by pointing your browser at https://login.mailguard.com.au



MailGuard - Microsoft Internet Explorer

Please log in

Username

Yourname

Password

****

Forgotten your password? Click here.

At this point, you will notice that a “key” will appear in the bottom right hand corner of your browser. This means that everything you now do is secure, and the username and passwords that you enter cannot be viewed by anyone over the Internet.

At this point, please enter your selected Username and Password as indicated on your initial application.

3.3 Forgotten Password

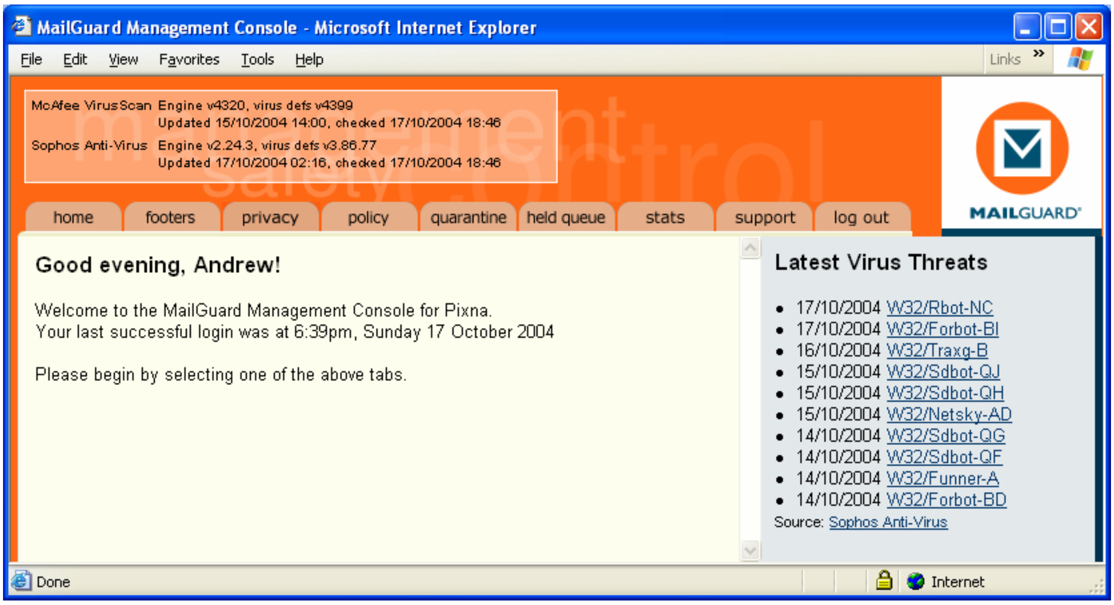
If you have forgotten your password, enter your Username in the Username field, and click on “Forgotten your password? Click here”, and a new password will be emailed to your email address.

As soon as you login with your new password, you will be prompted to change your password for security reasons.

If you have forgotten both your username and password, please contact:

Pacific Internet Support desk on 13 36 19

3.4 Welcome to CleanMail



McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 18:46
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 18:46

Good evening, Andrew!

Welcome to the MailGuard Management Console for Pixna.
Your last successful login was at 6:39pm, Sunday 17 October 2004

Please begin by selecting one of the above tabs.

Latest Virus Threats

- 17/10/2004 W32/Rbot-NC
- 17/10/2004 W32/Forbot-BI
- 16/10/2004 W32/Traxg-B
- 15/10/2004 W32/Sdbot-QJ
- 15/10/2004 W32/Sdbot-QH
- 15/10/2004 W32/Netsky-AD
- 14/10/2004 W32/Sdbot-QG
- 14/10/2004 W32/Sdbot-QF
- 14/10/2004 W32/Funner-A
- 14/10/2004 W32/Forbot-BD

Source: Sophos Anti-Virus

When you first login to CleanMail you are presented with the CleanMail Management console.

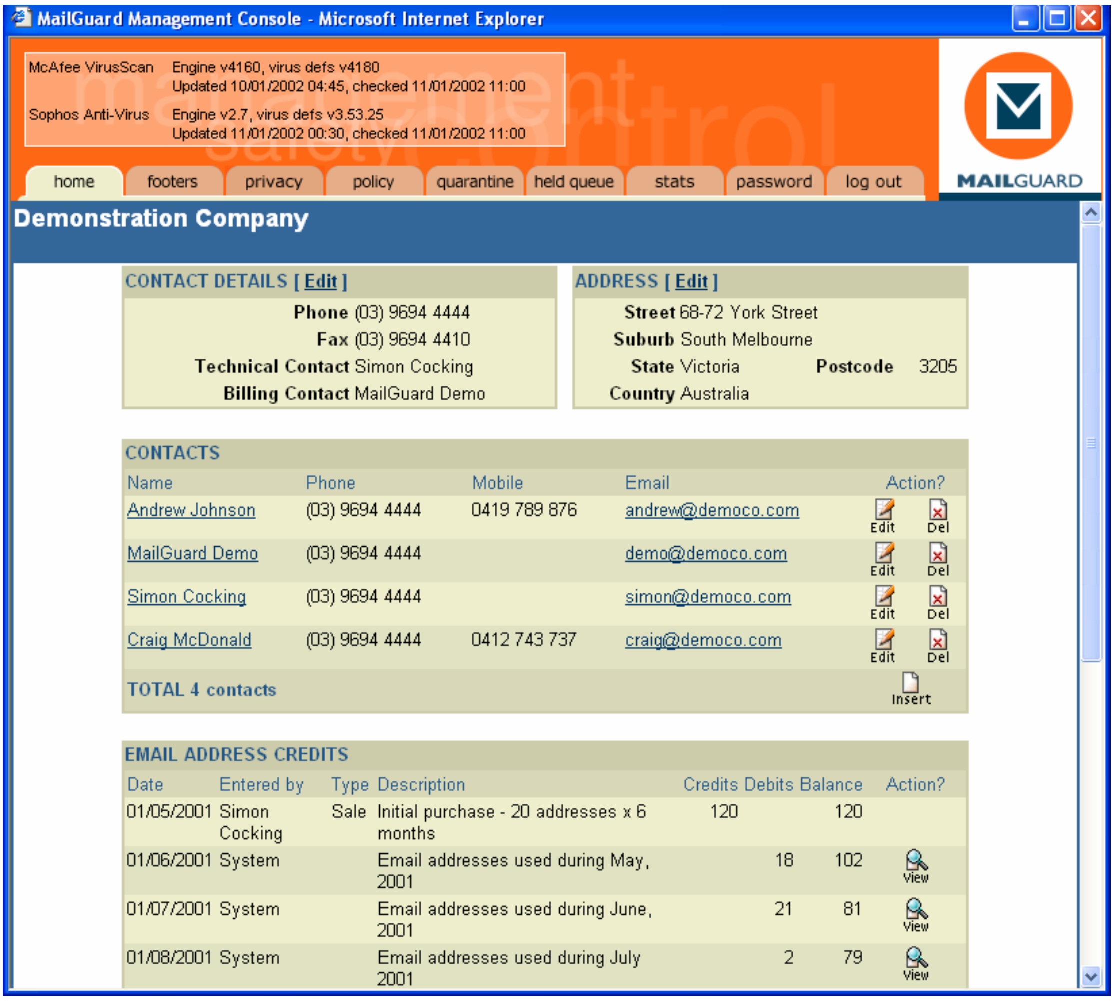
In the top left corner, you will see details and information of the frontline anti-virus software that CleanMail is utilising to filter your email, and when it was last updated and checked.

Below this, is your welcome message on the left, with current release viruses listed to the right – you may click on any of these to find out more about the virus.

CleanMail is operated largely through a tabbed menu system that works similar to a web page menu.

By moving the cursor over “**home, footers, privacy, policy, quarantine, held queue, stats, support and logout**” you will be provided with pop-up assistance on where each of these areas will take you.

3.5 Home – Information about you



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 11:00

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 11:00

Demonstration Company

CONTACT DETAILS [Edit]

Phone (03) 9694 4444
Fax (03) 9694 4410
Technical Contact Simon Cocking
Billing Contact MailGuard Demo

ADDRESS [Edit]

Street 68-72 York Street
Suburb South Melbourne
State Victoria **Postcode** 3205
Country Australia

CONTACTS

Name	Phone	Mobile	Email	Action?
Andrew Johnson	(03) 9694 4444	0419 789 876	andrew@democo.com	Edit Del
MailGuard Demo	(03) 9694 4444		demo@democo.com	Edit Del
Simon Cocking	(03) 9694 4444		simon@democo.com	Edit Del
Craig McDonald	(03) 9694 4444	0412 743 737	craig@democo.com	Edit Del
TOTAL 4 contacts				Insert

EMAIL ADDRESS CREDITS

Date	Entered by	Type	Description	Credits	Debits	Balance	Action?
01/05/2001	Simon Cocking	Sale	Initial purchase - 20 addresses x 6 months	120		120	
01/06/2001	System		Email addresses used during May, 2001		18	102	View
01/07/2001	System		Email addresses used during June, 2001		21	81	View
01/08/2001	System		Email addresses used during July 2001		2	79	View

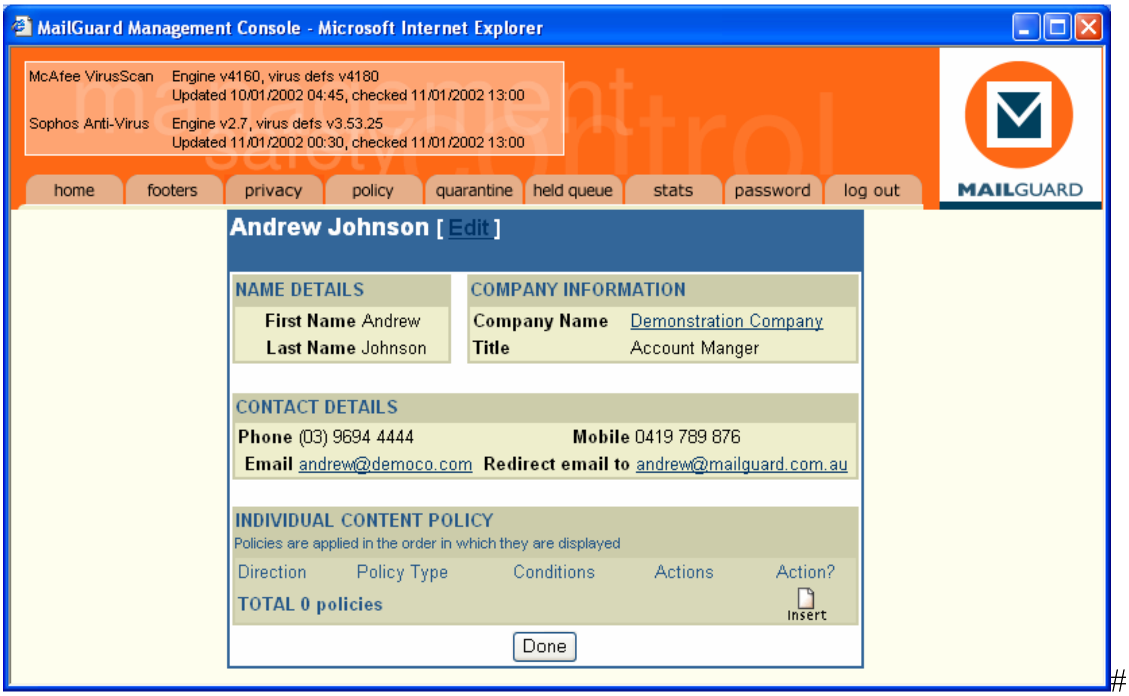
By selecting **home** from the menu bar, you are able to access information about your account. This includes phone number, address and your key contact people. You may make changes to this information by selecting “Edit” in the area that you wish to update.

#

3.5.1 Individual Contacts

By selecting the link of the **name** of the CONTACT in this page, you may then make changes, and set individual policies for this contact. It should be noted that individual policies may only be configured on people who you have setup as a contact.

#



MailGuard Management Console - Microsoft Internet Explorer

McAfee VirusScan	Engine v4160, virus defs v4180 Updated 10/01/2002 04:45, checked 11/01/2002 13:00
Sophos Anti-Virus	Engine v2.7, virus defs v3.53.25 Updated 11/01/2002 00:30, checked 11/01/2002 13:00

Andrew Johnson [Edit]

NAME DETAILS

First Name Andrew
Last Name Johnson

COMPANY INFORMATION

Company Name Demonstration Company
Title Account Manger

CONTACT DETAILS

Phone (03) 9694 4444 Mobile 0419 789 876
Email andrew@democo.com Redirect email to andrew@mailguard.com.au

INDIVIDUAL CONTENT POLICY

Policies are applied in the order in which they are displayed

Direction	Policy Type	Conditions	Actions	Action?
TOTAL 0 policies				Insert

#

#

Once the contact has been selected, in this case “Andrew Johnson”, you may then elect to “Edit” their details or proceed to [Insert] a new policy that applies to this contact individually. See section 3.7 and Section 4 for further information of the setup of policies.

#

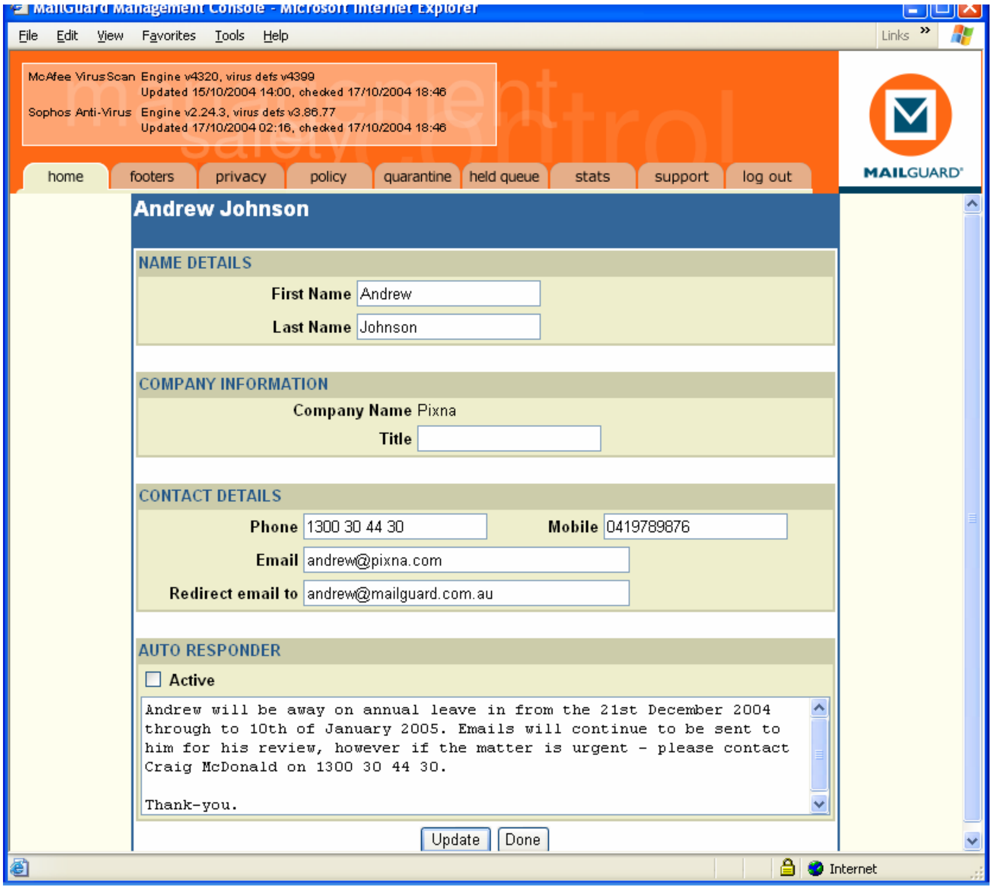
#

#

#

3.5.2 Redirect email to

The “redirect” function within CleanMail allows you to change the delivery point of your email to a different address. By selected “Edit” from the individual contact you are able to make changes to the details of your contacts, as well as the redirect destination.
#



McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 18:46
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 18:46

Andrew Johnson

NAME DETAILS

First Name: Andrew
Last Name: Johnson

COMPANY INFORMATION

Company Name Pixna
Title:

CONTACT DETAILS

Phone: 1300 30 44 30 Mobile: 0419789876
Email: andrew@pixna.com
Redirect email to: andrew@mailguard.com.au

AUTO RESPONDER

□ Active

```
Andrew will be away on annual leave in from the 21st December 2004
through to 10th of January 2005. Emails will continue to be sent to
him for his review, however if the matter is urgent - please contact
Craig McDonald on 1300 30 44 30.

Thank-you.
```
#

#
This example shows that all mail that is sent to andrew@pixna.com is actually re-routed directly to andrew@CleanMail.com.au.

3.5.3 Auto Responders

The Auto responder function is configurable either by domain, or by individual contact. In this case, an auto responder has been configured to automatically send an email back to anyone that sends an email to this contact, stating that the person is ‘on leave until the 10th of January 2005’.#

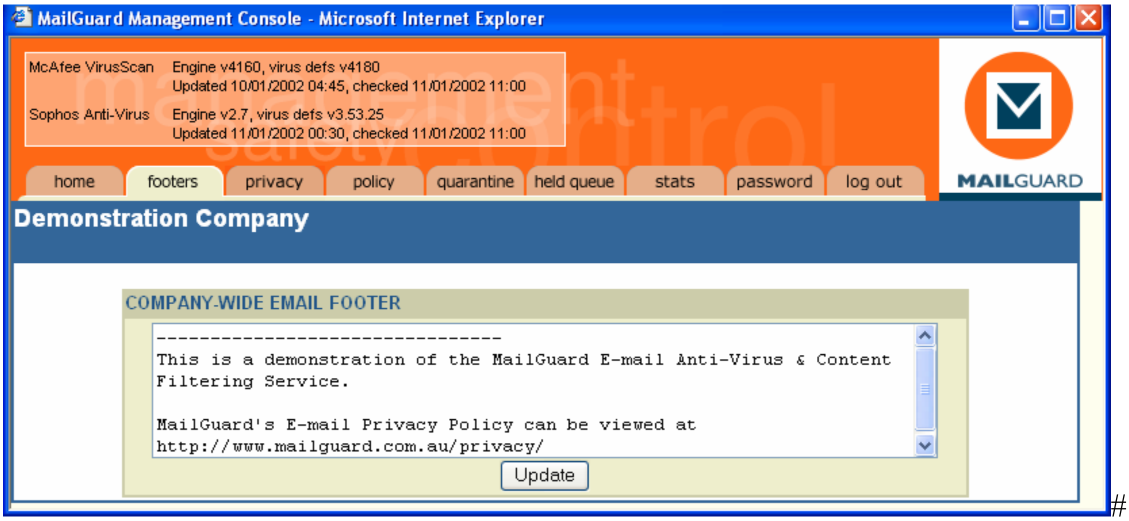
3.5.4 Email Address Credits

The email address credits displays your CleanMail usage and payments history. This is similar to looking at a bank statement and describes how many valid email users you have been billed for each month.

#

3.6 Footers

The **footers** area of the management console allows you to set a”Company-Wide” footer for all organisations that are within your company. This will apply to every domain that is being managed by your management console.



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 11:00

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 11:00

Demonstration Company

COMPANY-WIDE EMAIL FOOTER

```
--------------------------------
This is a demonstration of the MailGuard E-mail Anti-Virus & Content
Filtering Service.

MailGuard's E-mail Privacy Policy can be viewed at
http://www.mailguard.com.au/privacy/
```

#

#

#

#

3.7 Privacy

With the changes to the Australian Privacy Act 2000, which became law on the 21st of December 2001 – there are many new requirements for Australian organisations regarding the way they communicate with both individuals and companies.

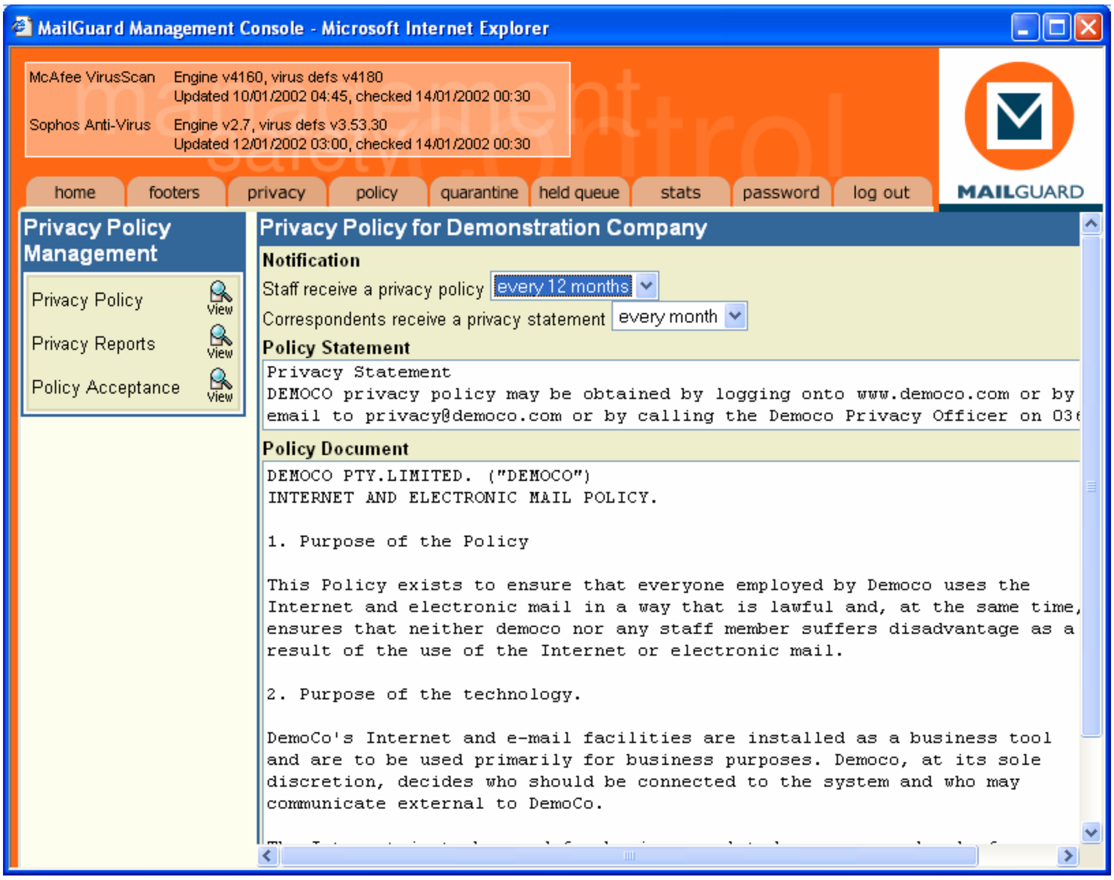
There are essentially three key areas where CleanMail assists your organisation in being compliant with the act, as well as providing a convenient tool to establish an understanding of how email and the Internet should be used within your organisation.

1) **Your staff**: CleanMail allows you to upload a "Privacy Policy" which may also contain your "Internet and email usage policy". This policy may be configured to automatically distribute via email to each of your staff the when they first receive email during a period of time (monthly, 3, 6, 12 monthly etc). If they receive the policy and agree with it – they should click the reply button.

2) **Your business correspondents**: According to the amendments to the privacy act, every person that sends an email to your organisation should see your "Privacy Statement". CleanMail automates this process by sending a copy of your "Privacy Statement" the first time a person sends an email to your organisation during a specific period of time.

3) **Reporting:** CleanMail provides reports as to who has received these policies and statements, as well as if they have accepted/responded to them. CleanMail also provides the ability to send any of your staff or correspondents a list of all the information that CleanMail has stored with regard to their email usage, as is required in the "Act".

3.7.1 Upload Privacy Policy



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 14/01/2002 00:30

Sophos Anti-Virus Engine v2.7, virus defs v3.53.30
Updated 12/01/2002 03:00, checked 14/01/2002 00:30

Privacy Policy Management

- Privacy Policy
- Privacy Reports
- Policy Acceptance

Privacy Policy for Demonstration Company

Notification

Staff receive a privacy policy: every 12 months

Correspondents receive a privacy statement: every month

Policy Statement

```
Privacy Statement
DEMOCO privacy policy may be obtained by logging onto www.democo.com or by
email to privacy@democo.com or by calling the Democo Privacy Officer on 03
```

Policy Document

```
DEMOCO PTY.LIMITED. ("DEMOCO")
INTERNET AND ELECTRONIC MAIL POLICY.

1. Purpose of the Policy

This Policy exists to ensure that everyone employed by Democo uses the
Internet and electronic mail in a way that is lawful and, at the same time,
ensures that neither democo nor any staff member suffers disadvantage as a
result of the use of the Internet or electronic mail.

2. Purpose of the technology.

DemoCo's Internet and e-mail facilities are installed as a business tool
and are to be used primarily for business purposes. Democo, at its sole
discretion, decides who should be connected to the system and who may
communicate external to DemoCo.
```

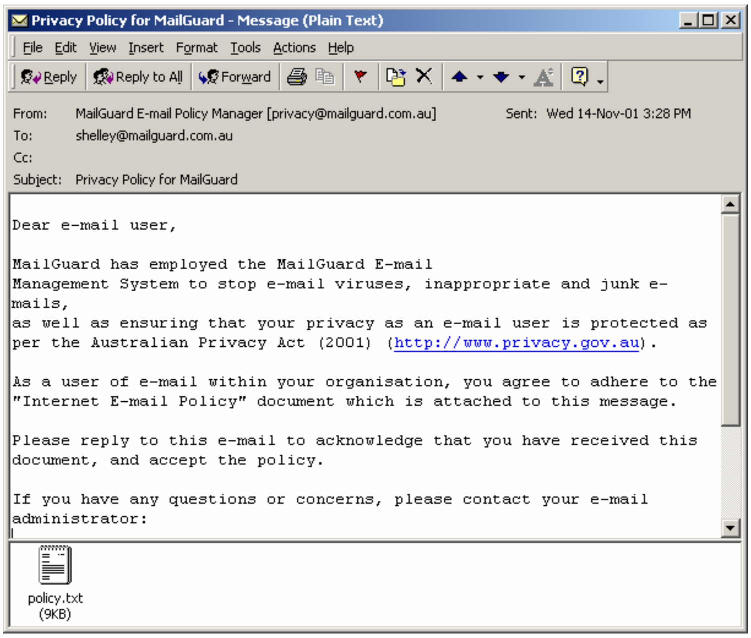
The first step to configuring your privacy compliance management within CleanMail is to upload your organisations “Email Privacy Policy” and “Email Privacy Statement” onto the CleanMail system from the management console.

This can be achieved by entering the **Privacy tab**, and selecting “Privacy Policy”. Your policy & statement may be pasted into this area.

Once your organisations “Email Privacy Policy” has been loaded into CleanMail, you may then select whether you wish to automatically send this document to your employees every month, three months, six months or annually.

After this selection has been made, CleanMail will automatically send your “Email Privacy Policy” to your employees at the interval selected.

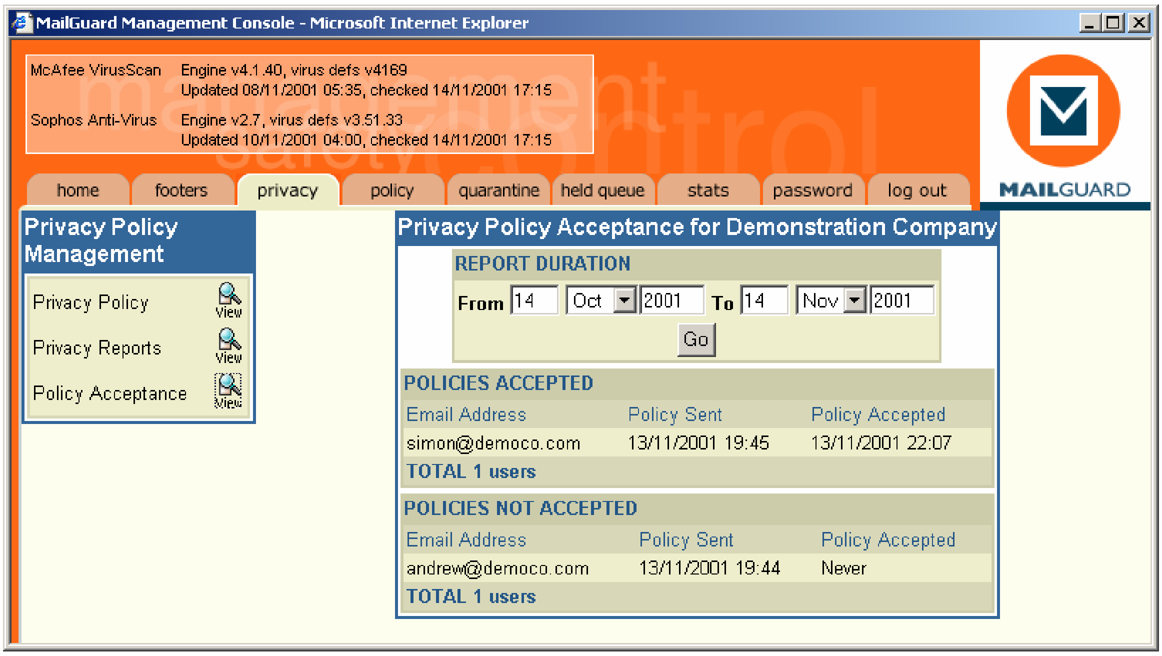
Once your employees receive this policy, they may elect to “reply” to the messages, and hence show that they have read your organisations “Email Privacy Policy”.


Privacy Policy for MailGuard - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
policy.txt
(9KB)

From: MailGuard E-mail Policy Manager [privacy@mailguard.com.au]
Sent: Wed 14-Nov-01 3:28 PM
To: shelley@mailguard.com.au
Cc:
Subject: Privacy Policy for MailGuard

```
Dear e-mail user,

MailGuard has employed the MailGuard E-mail
Management System to stop e-mail viruses, inappropriate and junk e-
mails,
as well as ensuring that your privacy as an e-mail user is protected as
per the Australian Privacy Act (2001) (http://www.privacy.gov.au).

As a user of e-mail within your organisation, you agree to adhere to the
"Internet E-mail Policy" document which is attached to this message.

Please reply to this e-mail to acknowledge that you have received this
document, and accept the policy.

If you have any questions or concerns, please contact your e-mail
administrator:
```

3.7.2 Acceptance of Privacy Policy



McAfee VirusScan Engine v4.1.40, virus defs v4169
Updated 08/11/2001 05:35, checked 14/11/2001 17:15

Sophos Anti-Virus Engine v2.7, virus defs v3.51.33
Updated 10/11/2001 04:00, checked 14/11/2001 17:15

Privacy Policy Acceptance for Demonstration Company

REPORT DURATION

From 14 Oct 2001 To 14 Nov 2001

POLICIES ACCEPTED

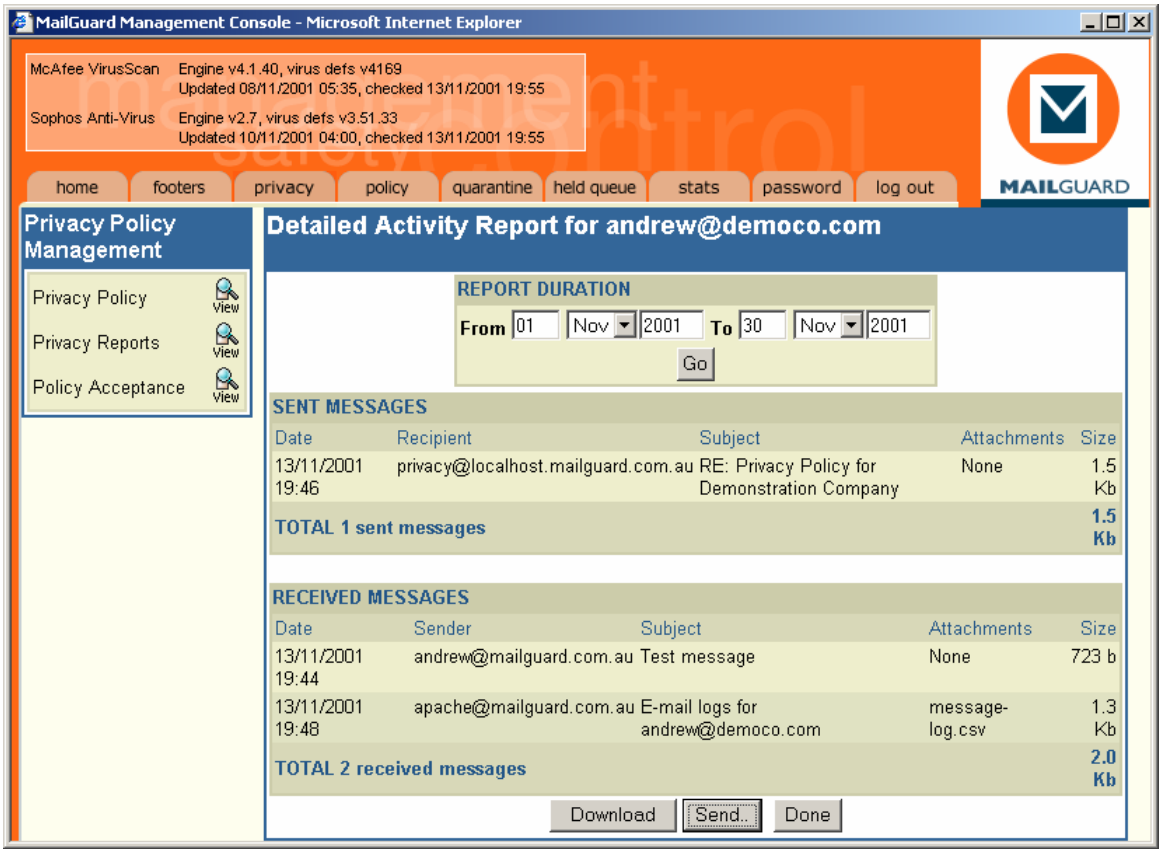
Email Address	Policy Sent	Policy Accepted
simon@democo.com	13/11/2001 19:45	13/11/2001 22:07
TOTAL 1 users		

POLICIES NOT ACCEPTED

Email Address	Policy Sent	Policy Accepted
andrew@democo.com	13/11/2001 19:44	Never
TOTAL 1 users		

As the CleanMail Administrator for your organisation, you may at any time log in to your CleanMail Management Console, and produce a report of your employees detailing who has, and hasn’t accepted your “Email Privacy Policy”. This is accessed by selecting “Privacy Reports”.

3.7.3 Response to a Request for logged Information



McAfee VirusScan Engine v4.1.40, virus defs v4169
Updated 08/11/2001 05:35, checked 13/11/2001 19:55

Sophos Anti-Virus Engine v2.7, virus defs v3.51.33
Updated 10/11/2001 04:00, checked 13/11/2001 19:55

Privacy Policy Management

Detailed Activity Report for andrew@democo.com

REPORT DURATION

From 01 Nov 2001 To 30 Nov 2001

SENT MESSAGES

Date	Recipient	Subject	Attachments	Size
13/11/2001 19:46	privacy@localhost.mailguard.com.au	RE: Privacy Policy for Demonstration Company	None	1.5 Kb
TOTAL 1 sent messages				**1.5 Kb**

RECEIVED MESSAGES

Date	Sender	Subject	Attachments	Size
13/11/2001 19:44	andrew@mailguard.com.au	Test message	None	723 b
13/11/2001 19:48	apache@mailguard.com.au	E-mail logs for andrew@democo.com	message-log.csv	1.3 Kb
TOTAL 2 received messages				**2.0 Kb**

The amendment to the Act also allows your employees to request a copy of any information or statistics that you acquire from them during the course of business such as email logs, and usage.

CleanMail simplifies this process by allowing you to select the person’s email address from the CleanMail Management Console, and pressing the “Send” button. This instructs CleanMail to email a copy of the complete logs that CleanMail has stored on your employees email traffic and statistics, directly to them.

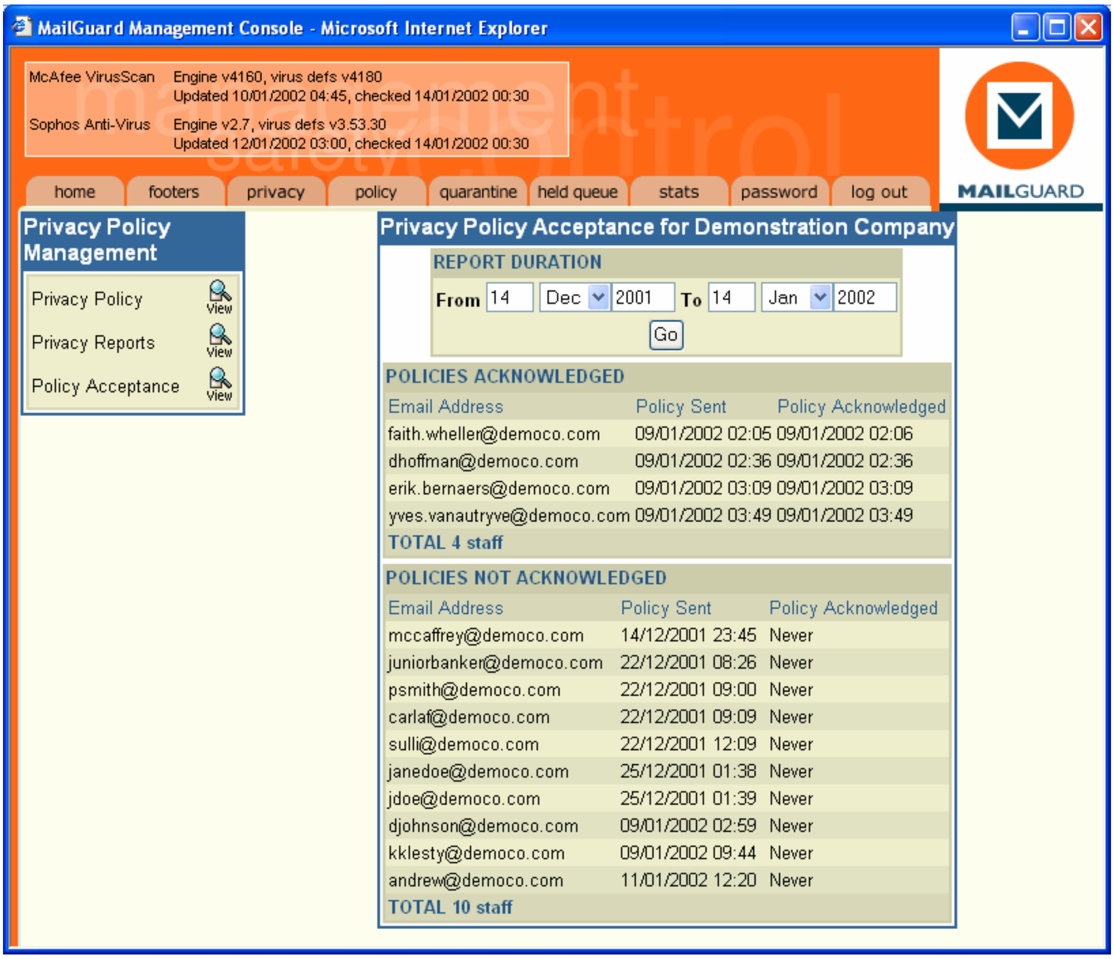
#

3.7.4 External email policy management

Every person who sends email into your organisation requires a copy of your email privacy statement – CleanMail intelligently automates this process for your business.

The first time a person sends email to your organisation they will receive a copy of your policy directly from CleanMail. Thereafter, CleanMail has registered that this person has your policy, and will not require further copies sent.

A report may be generated at any time allowing you to check if an individual has been sent your email policy or not. This process is refreshed every month in order to provide a reasonable, but not overbearing communications with the people corresponding with your organisation.



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 14/01/2002 00:30

Sophos Anti-Virus Engine v2.7, virus defs v3.53.30
Updated 12/01/2002 03:00, checked 14/01/2002 00:30

Privacy Policy Acceptance for Demonstration Company

REPORT DURATION

From 14 Dec 2001 To 14 Jan 2002

POLICIES ACKNOWLEDGED

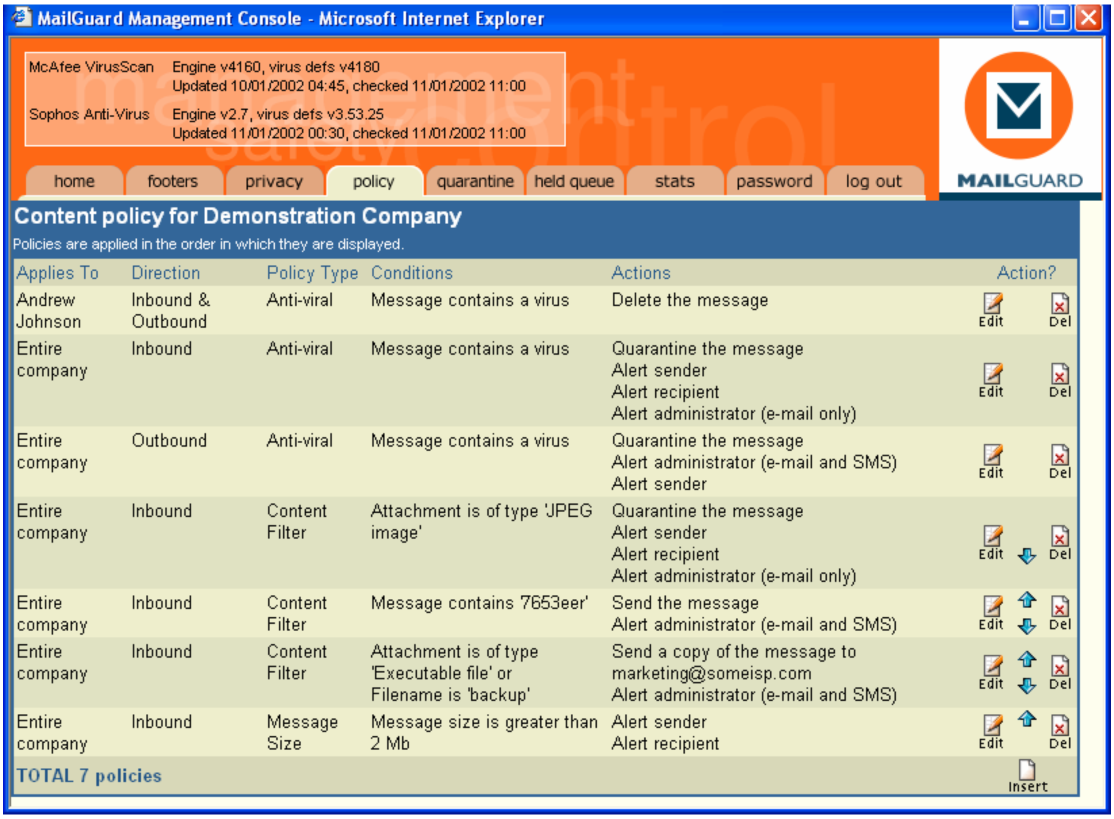
Email Address	Policy Sent	Policy Acknowledged
faith.wheller@democo.com	09/01/2002 02:05	09/01/2002 02:06
dhoffman@democo.com	09/01/2002 02:36	09/01/2002 02:36
erik.bernaers@democo.com	09/01/2002 03:09	09/01/2002 03:09
yves.vanautryve@democo.com	09/01/2002 03:49	09/01/2002 03:49
TOTAL 4 staff		

POLICIES NOT ACKNOWLEDGED

Email Address	Policy Sent	Policy Acknowledged
mccaffrey@democo.com	14/12/2001 23:45	Never
juniorbanker@democo.com	22/12/2001 08:26	Never
psmith@democo.com	22/12/2001 09:00	Never
carlaf@democo.com	22/12/2001 09:09	Never
sulli@democo.com	22/12/2001 12:09	Never
janedoe@democo.com	25/12/2001 01:38	Never
jdoe@democo.com	25/12/2001 01:39	Never
djohnson@democo.com	09/01/2002 02:59	Never
kklesty@democo.com	09/01/2002 09:44	Never
andrew@democo.com	11/01/2002 12:20	Never
TOTAL 10 staff		

3.8 Policy

The **policy** section of the management console is where you create and edit global policies that affect all users in your company. For details on configuring rules and policies that apply to either individual email addresses or specific domains, please go to **Section 4.1.**



McAfee VirusScan	Engine v4160, virus defs v4180 Updated 10/01/2002 04:45, checked 11/01/2002 11:00
Sophos Anti-Virus	Engine v2.7, virus defs v3.53.25 Updated 11/01/2002 00:30, checked 11/01/2002 11:00

Content policy for Demonstration Company

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Andrew Johnson	Inbound & Outbound	Anti-viral	Message contains a virus	Delete the message	Edit Del
Entire company	Inbound	Anti-viral	Message contains a virus	Quarantine the message Alert sender Alert recipient Alert administrator (e-mail only)	Edit Del
Entire company	Outbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator (e-mail and SMS) Alert sender	Edit Del
Entire company	Inbound	Content Filter	Attachment is of type 'JPEG image'	Quarantine the message Alert sender Alert recipient Alert administrator (e-mail only)	Edit ↓ Del
Entire company	Inbound	Content Filter	Message contains '7653eer'	Send the message Alert administrator (e-mail and SMS)	Edit ↑↓ Del
Entire company	Inbound	Content Filter	Attachment is of type 'Executable file' or Filename is 'backup'	Send a copy of the message to marketing@someisp.com Alert administrator (e-mail and SMS)	Edit ↑↓ Del
Entire company	Inbound	Message Size	Message size is greater than 2 Mb	Alert sender Alert recipient	Edit ↑ Del
TOTAL 7 policies					Insert

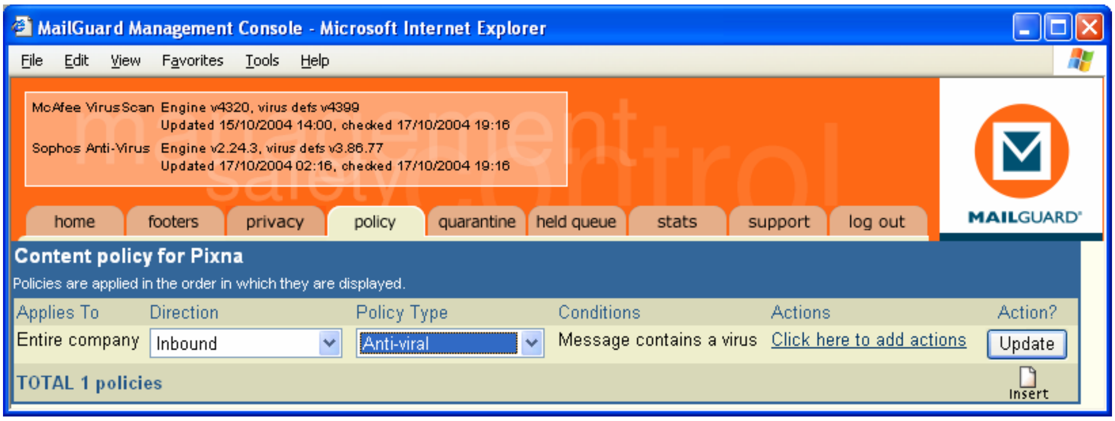
We begin by either editing [Edit] an existing policy, or inserting [Insert] a new policy. A policy is any rule that you wish to be applied to the email as it transits CleanMail. It should be noted that when email transits the CleanMail system, the policies **WILL ALWAYS BE APPLIED FROM TOP TO BOTTOM IN THE ORDER THAT THEY APPEAR IN THE POLICY EDITOR.**

3.8.1 Adding a new policy

Let’s begin with adding a policy that says:

“Applying to the whole company, delete all inbound viruses from entering my business, and notify me once a day of the items deleted”.

To create this, we first, click on “ Insert ” in the bottom right corner – to add a new policy.



MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 19:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 19:16

Content policy for Pixna

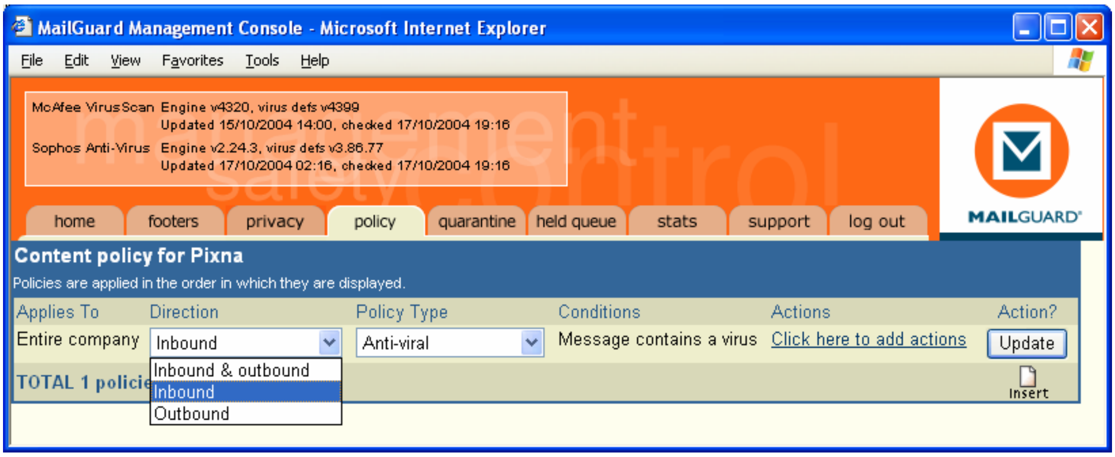
Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Click here to add actions	Update
TOTAL 1 policies					Insert

3.8.2 Applies to

In the left hand column (under “Applies To”), you will notice that “Entire Company” is listed, as this is a policy that applies to everyone. In the circumstance where you are editing a policy for either a domain or an individual then it would list either a domain or an individual person that this policy applies to (for domain or individual policies see section 4.1).

3.8.3 Direction


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD
Inbound & outbound
Inbound
Outbound
Update
Insert

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 19:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 19:16

Content policy for Pixna

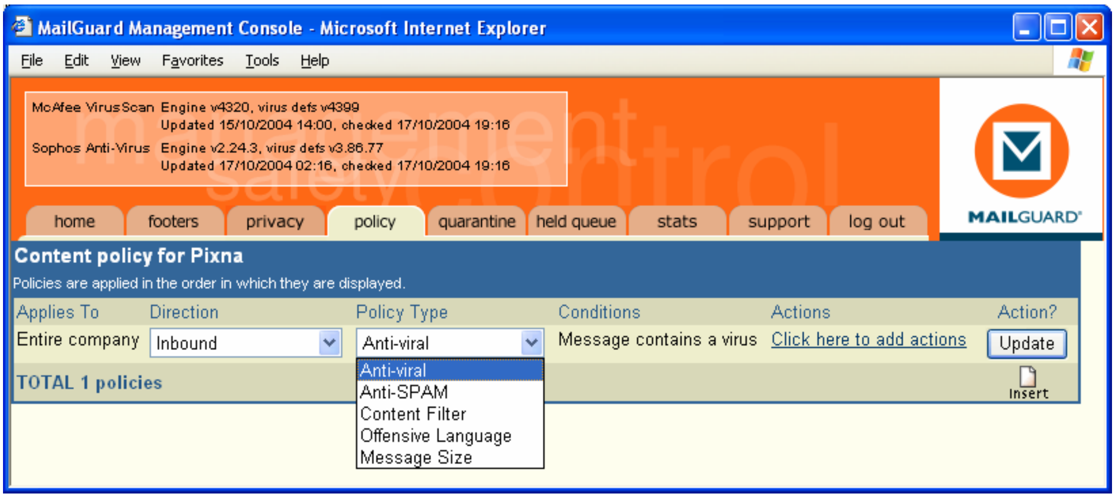
Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Click here to add actions	Update

TOTAL 1 policies

The next to be made is “Direction” – do you wish this policy to apply for all incoming email (inbound), email that your people send out (outbound) or all email (inbound and outbound). In this example we wish to setup a policy for “inbound”.

3.8.4 Policy Type


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD
Anti-viral
Anti-SPAM
Content Filter
Offensive Language
Message Size
Update
Insert

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 19:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 19:16

Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Click here to add actions	Update

TOTAL 1 policies

The next selection is “Policy Type”. There are five basic policy types with CleanMail.

1. Anti-viral
2. Anti-spam
3. Content Filtering
4. Offensive Language
5. Message Size

“Anti-Viral” is selected for the policy that we wish to apply here, however options 2, 3, 4 & 5 being “Anti-Spam”, “Content Filtering”, “Offensive

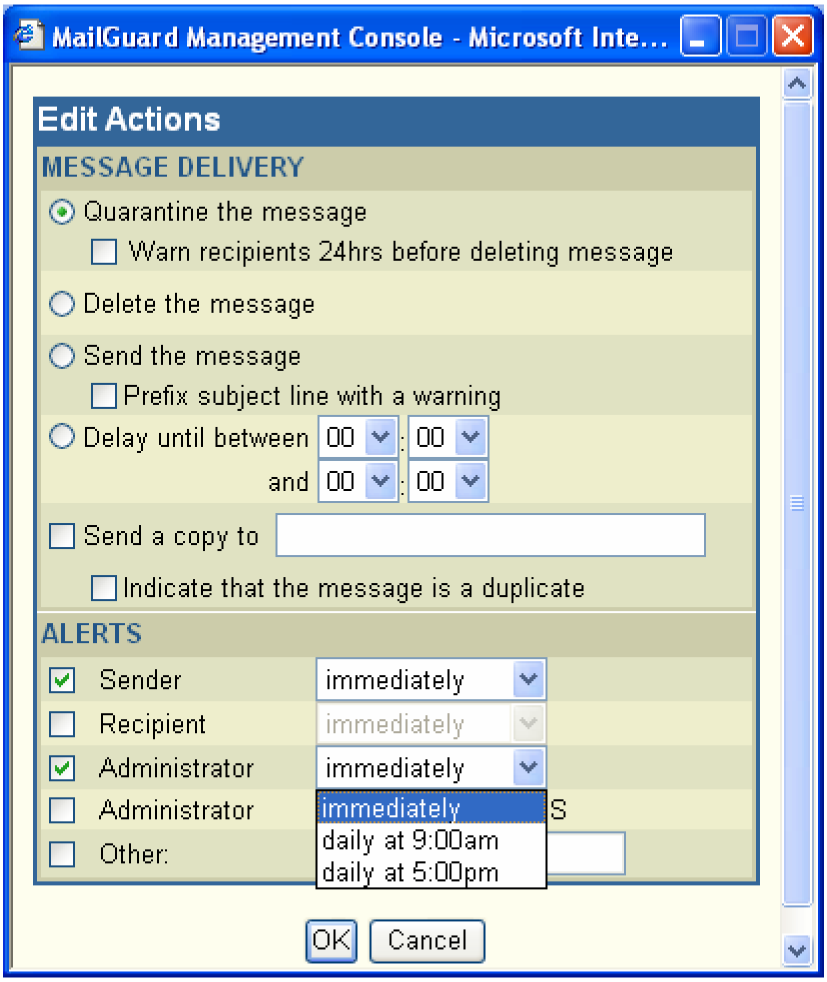
Language" and "Message Size" allow other different types of policies to be configured from this window. *(See Section 4: Setup & Management).*

We will select **Anti-Viral.**

After we have selected the "Direction", and the "Policy Type" the next thing that we need to consider is what do we wish to happen when CleanMail does find a virus?

3.8.5 Actions

This is when we need to click onto "Actions".



Edit Actions

MESSAGE DELIVERY

● Quarantine the message
□ Warn recipients 24hrs before deleting message
○ Delete the message
○ Send the message
□ Prefix subject line with a warning
○ Delay until between 00 : 00 and 00 : 00
□ Send a copy to
□ Indicate that the message is a duplicate

ALERTS

☑ Sender immediately
□ Recipient immediately
☑ Administrator immediately
□ Administrator S
□ Other:

immediately
daily at 9:00am
daily at 5:00pm

"Actions" allow you to tell CleanMail exactly what you wish it to do when the policy that you have set is met.

The options are as follows:

Quarantine Message: Do not allow the message through. Place it into a quarantine area (at CleanMail) where you may then login at a later stage, and decide whether this message should be deleted or sent on to the intended recipient. Usually the Quarantine message option is used in conjunction with an “Alert” to the administrator (being you) so that you are aware that there is a message in quarantine requiring your attention. Quarantined messages will automatically be deleted after 7 days.

CleanMail also apply a quota to the quarantine of 2000 messages. If your quarantined messages approach this quota, you will be notified immediately via email and sms (optional).

You may also select to notify the “alert recipients” at the 6th day, saying that the message is about to be deleted from quarantine.

Send the Message: This allows the message to be sent – this would not normally be appropriate for an anti-viral rule, however may be useful if you wish to be made aware when a certain file is being transferred, or emails are being received by certain people, but are not concerned about holding it up within the quarantine.

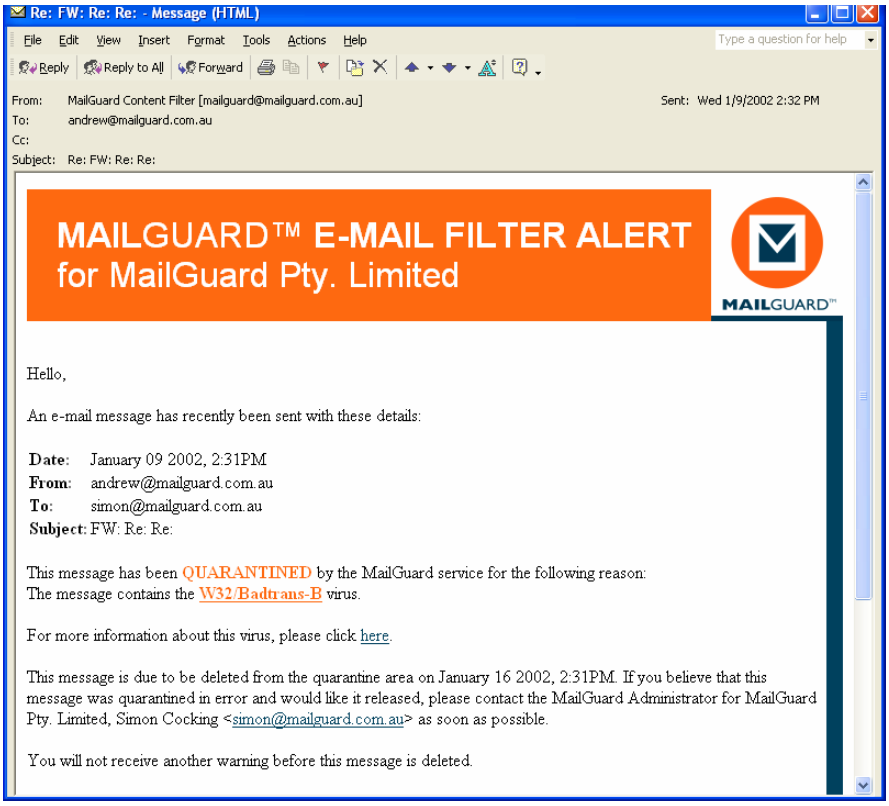
Delay the Message: This action is very useful for “Message Size” or “MP3” policies whereby you may wish to delay large emails for transmission outside of peak or office hours.

Send a Copy to: This action allows the email to transit CleanMail in the normal way, however, to also send a copy or alert of the email to a specific email address.

3.8.6 Alerts

Alerts may be configured as either “Immediate” or “Digest – to be delivered once a day at either 9am or 5pm”.

Once you have decided what you wish CleanMail to do with your message if it meets your policy criteria, the next stage is to decide whom you wish to tell about this.


Re: FW: Re: Re: - Message (HTML)
File Edit View Insert Format Tools Actions Help
Type a question for help
Reply
Reply to All
Forward
MAILGUARD™

From: MailGuard Content Filter [mailguard@mailguard.com.au]
To: andrew@mailguard.com.au
Cc:
Subject: Re: FW: Re: Re:
Sent: Wed 1/9/2002 2:32 PM

MAILGUARD™ E-MAIL FILTER ALERT
for MailGuard Pty. Limited

Hello,

An e-mail message has recently been sent with these details:

Date: January 09 2002, 2:31PM
From: andrew@mailguard.com.au
To: simon@mailguard.com.au
Subject: FW: Re: Re:

This message has been QUARANTINED by the MailGuard service for the following reason:
The message contains the **W32/Badtrans-B** virus.

For more information about this virus, please click here.

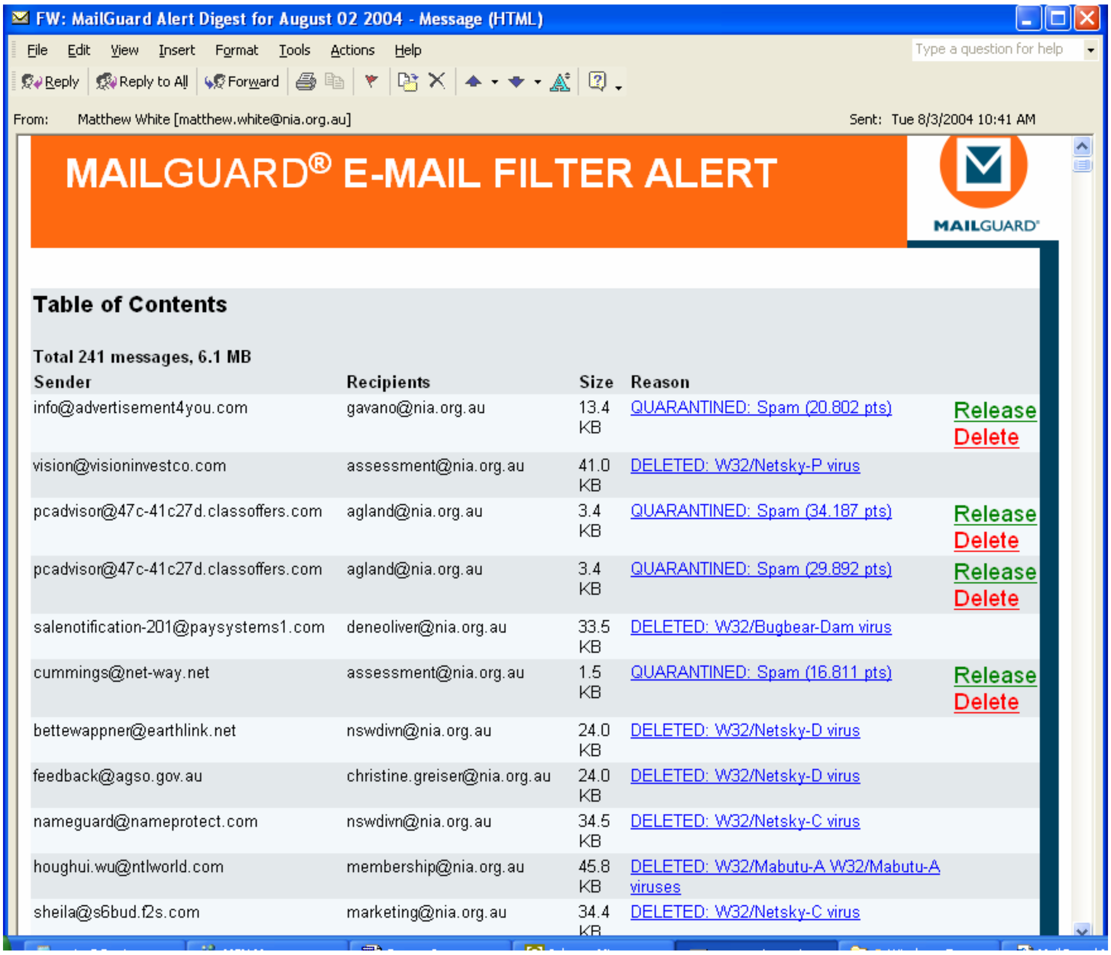
This message is due to be deleted from the quarantine area on January 16 2002, 2:31PM. If you believe that this message was quarantined in error and would like it released, please contact the MailGuard Administrator for MailGuard Pty. Limited, Simon Cocking <simon@mailguard.com.au> as soon as possible.

You will not receive another warning before this message is deleted.

By selecting various alerts, you are able to notify any combination of sender, recipient, other email address, administrator or SMS on a digital cellular phone when your conditions have been met. In the default anti-viral policy, we would usually recommend the notification be to the Sender *(so that they know that they have accidentally sent you a virus – we will not notify the sender on viruses that are known to forge their sender addresses),* the recipient [Digest] *(so that the person within your company is aware that someone is trying to send them an email – but it had a virus in it and has been quarantined)* and the Administrator [Digest] *(so that you are aware that a virus has attempted to enter your network, and been stopped).*

3.8.7 Administrator Digest Alerts

The Administrator alerts have the added function of being able to Delete/Release the quarantined messages by clicking on the links within the alert message.



From: Matthew White [matthew.white@nia.org.au]

Sent: Tue 8/3/2004 10:41 AM

MAILGUARD® E-MAIL FILTER ALERT

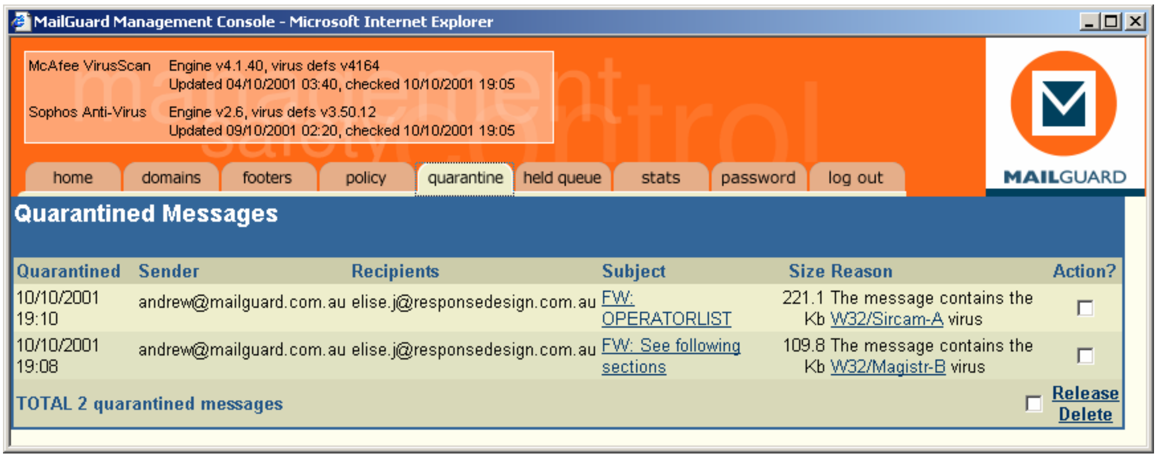
Table of Contents

Total 241 messages, 6.1 MB

Sender	Recipients	Size	Reason	
info@advertisement4you.com	gavano@nia.org.au	13.4 KB	QUARANTINED: Spam (20.802 pts)	Release Delete
vision@visioninvestco.com	assessment@nia.org.au	41.0 KB	DELETED: W32/Netsky-P virus	
pcadvisor@47c-41c27d.classoffers.com	agland@nia.org.au	3.4 KB	QUARANTINED: Spam (34.187 pts)	Release Delete
pcadvisor@47c-41c27d.classoffers.com	agland@nia.org.au	3.4 KB	QUARANTINED: Spam (29.892 pts)	Release Delete
salenotification-201@paysystems1.com	deneoliver@nia.org.au	33.5 KB	DELETED: W32/Bugbear-Dam virus	
cummings@net-way.net	assessment@nia.org.au	1.5 KB	QUARANTINED: Spam (16.811 pts)	Release Delete
bettewappner@earthlink.net	nswdivn@nia.org.au	24.0 KB	DELETED: W32/Netsky-D virus	
feedback@agso.gov.au	christine.greiser@nia.org.au	24.0 KB	DELETED: W32/Netsky-D virus	
nameguard@nameprotect.com	nswdivn@nia.org.au	34.5 KB	DELETED: W32/Netsky-C virus	
houghui.wu@ntlworld.com	membership@nia.org.au	45.8 KB	DELETED: W32/Mabutu-A W32/Mabutu-A viruses	
sheila@s6bud.f2s.com	marketing@nia.org.au	34.4 KB	DELETED: W32/Netsky-C virus	

By click on the “Release” button, you may elect to release the message directly from the Email Filter Alert rather than actually logging into the quarantine area.

3.9 Quarantine



McAfee VirusScan Engine v4.1.40, virus defs v4164
Updated 04/10/2001 03:40, checked 10/10/2001 19:05

Sophos Anti-Virus Engine v2.6, virus defs v3.50.12
Updated 09/10/2001 02:20, checked 10/10/2001 19:05

Quarantined Messages

Quarantined	Sender	Recipients	Subject	Size	Reason	Action?
10/10/2001 19:10	andrew@mailguard.com.au	elise.j@responsedesign.com.au	FW: OPERATORLIST	221.1 Kb	The message contains the W32/Sircam-A virus	☐
10/10/2001 19:08	andrew@mailguard.com.au	elise.j@responsedesign.com.au	FW: See following sections	109.8 Kb	The message contains the W32/Magistr-B virus	☐
TOTAL 2 quarantined messages						☐ Release Delete

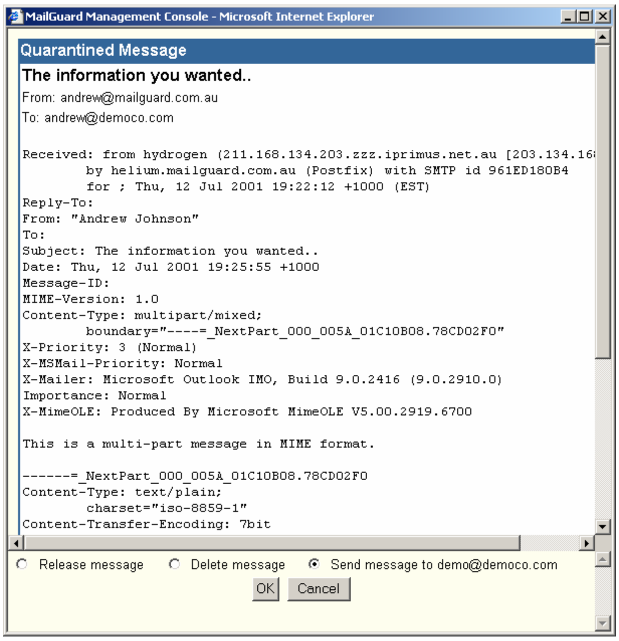
When email has been quarantined – you may view its status through the “**Quarantine**” tab on the management console. From this screen you can see the sender, recipient, subject, reason and decide what you wish to do with this message.

Also, from this screen you may elect to either “release” (virus messages may not be released) or delete the message.

If you have not released or deleted this message after six days you may be optionally reminded that on the seventh day, the message will automatically be deleted.

3.9.1 View the Message

By clicking on the “Subject” section of the quarantine line, you are able to view the message **safely** over the Internet. This allows you to better establish whether this message is required, and the nature of the message.



The information you wanted..

From: andrew@mailguard.com.au

To: andrew@democo.com

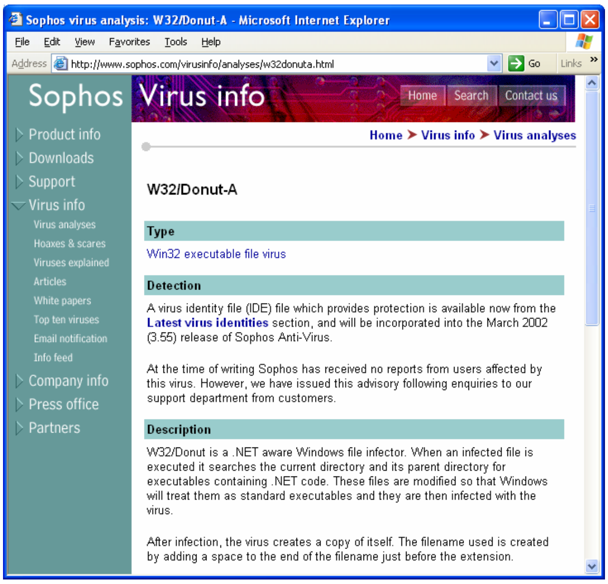
```
Received: from hydrogen (211.168.134.203.zzz.iprimus.net.au [203.134.16
        by helium.mailguard.com.au (Postfix) with SMTP id 961ED180B4
        for ; Thu, 12 Jul 2001 19:22:12 +1000 (EST)
Reply-To:
From: "Andrew Johnson"
To:
Subject: The information you wanted..
Date: Thu, 12 Jul 2001 19:25:55 +1000
Message-ID:
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_005A_01C10B08.78CD02F0"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

This is a multi-part message in MIME format.

------=_NextPart_000_005A_01C10B08.78CD02F0
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
```

○ Release message ○ Delete message ● Send message to demo@democo.com

From this screen, you may also elect to send a copy of the message to yourself for further evaluation or action.

3.9.2 Find out about the virus

In the case that the message has been quarantined as it has a virus – the virus name will be highlighted. By clicking on the virus name information will appear.



http://www.sophos.com/virusinfo/analyses/w32donuta.html

W32/Donut-A

Type

Win32 executable file virus

Detection

A virus identity file (IDE) file which provides protection is available now from the **Latest virus identities** section, and will be incorporated into the March 2002 (3.55) release of Sophos Anti-Virus.

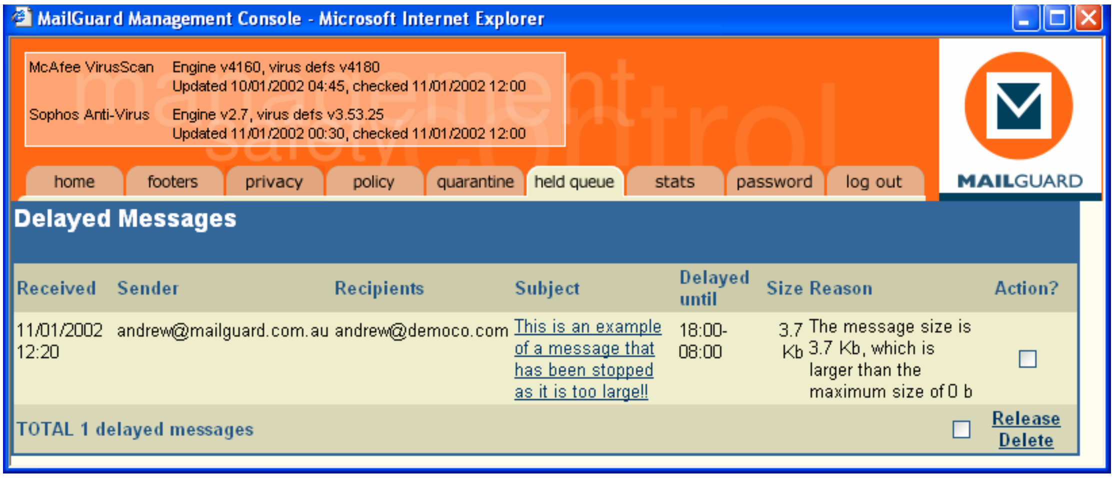
At the time of writing Sophos has received no reports from users affected by this virus. However, we have issued this advisory following enquiries to our support department from customers.

Description

W32/Donut is a .NET aware Windows file infector. When an infected file is executed it searches the current directory and its parent directory for executables containing .NET code. These files are modified so that Windows will treat them as standard executables and they are then infected with the virus.

After infection, the virus creates a copy of itself. The filename used is created by adding a space to the end of the filename just before the extension.

3.10 Held Queue



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 12:00

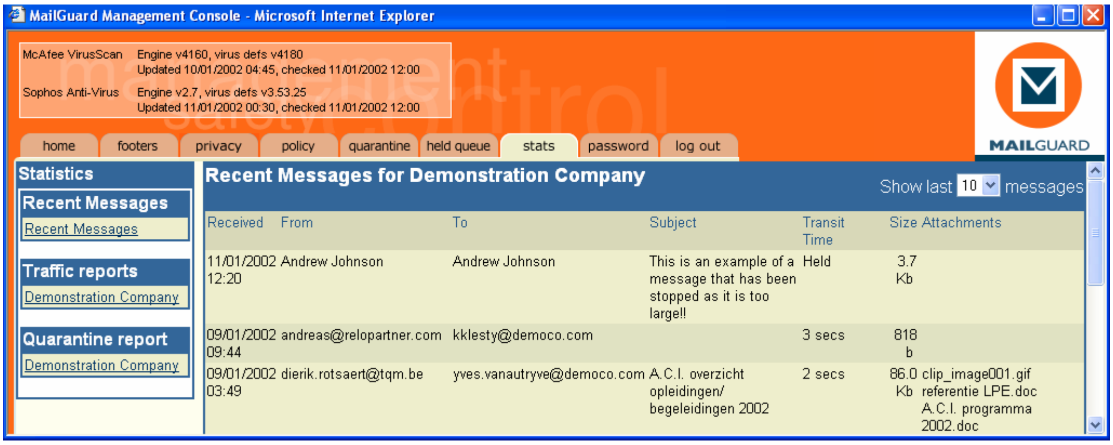
Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 12:00

Delayed Messages

Received	Sender	Recipients	Subject	Delayed until	Size	Reason	Action?
11/01/2002 12:20	andrew@mailguard.com.au	andrew@democo.com	This is an example of a message that has been stopped as it is too large!!	18:00-08:00	3.7 Kb	The message size is 3.7 Kb, which is larger than the maximum size of 0 b	□
TOTAL 1 delayed messages						□	Release Delete

The **help queue** is similar to Quarantine – except, that email that sits within the held queue will stay in this area until a specified time. The Held Queue is primarily used for organisations that wish to deliver "large" emails after-hours savings on off-peak Internet rates, and avoiding bandwidth disruption and congestion during business hours.

3.11 Stats



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 12:00

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 12:00

Recent Messages for Demonstration Company

Show last 10 messages

Received	From	To	Subject	Transit Time	Size	Attachments
11/01/2002 12:20	Andrew Johnson	Andrew Johnson	This is an example of a message that has been stopped as it is too large!!	Held	3.7 Kb	
09/01/2002 09:44	andreas@relopartner.com	kklesty@democo.com		3 secs	818 b	
09/01/2002 03:49	dierik.rotsaert@tqm.be	yves.vanautryve@democo.com	A.C.I. overzicht opleidingen/ begeleidingen 2002	2 secs	86.0 Kb	clip_image001.gif referentie LPE.doc A.C.I. programma 2002.doc

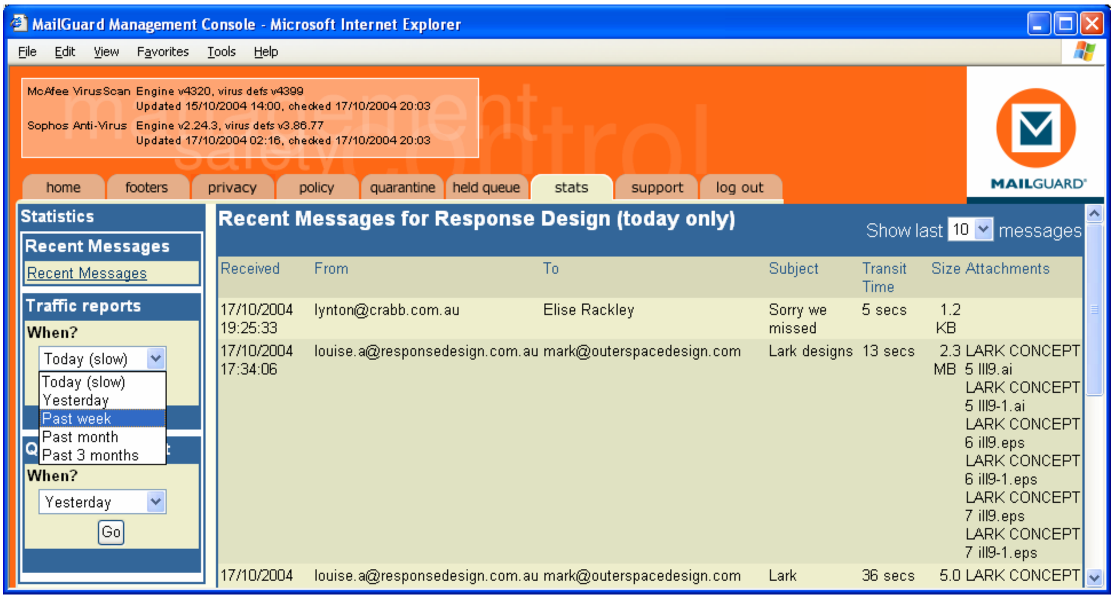
The **stats** tab on CleanMail provides valuable statistics of what is occurring with your organisations email.

The first link on the left hand side is “Recent Messages” which provides a window to what email is coming and going in real-time for the last day.

The details on the screen provide the following information:

Received: Date and time that the message was received by CleanMail.
From: The envelope address of the person who sent the message.
To: The email address of the person who the message was sent to.
Subject: The subject of the email.
Transit Time: The amount of time the message took to go through CleanMail (and be checked for viruses and the policies that apply to it).
Size: The size of the email.
Attachment: The names of any attachments to the email.

3.11.1 Traffic Report


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD
Statistics
Recent Messages
Traffic reports
When?
Today (slow)
Today (slow)
Yesterday
Past week
Past month
Past 3 months
When?
Yesterday
Go
Show last 10 messages

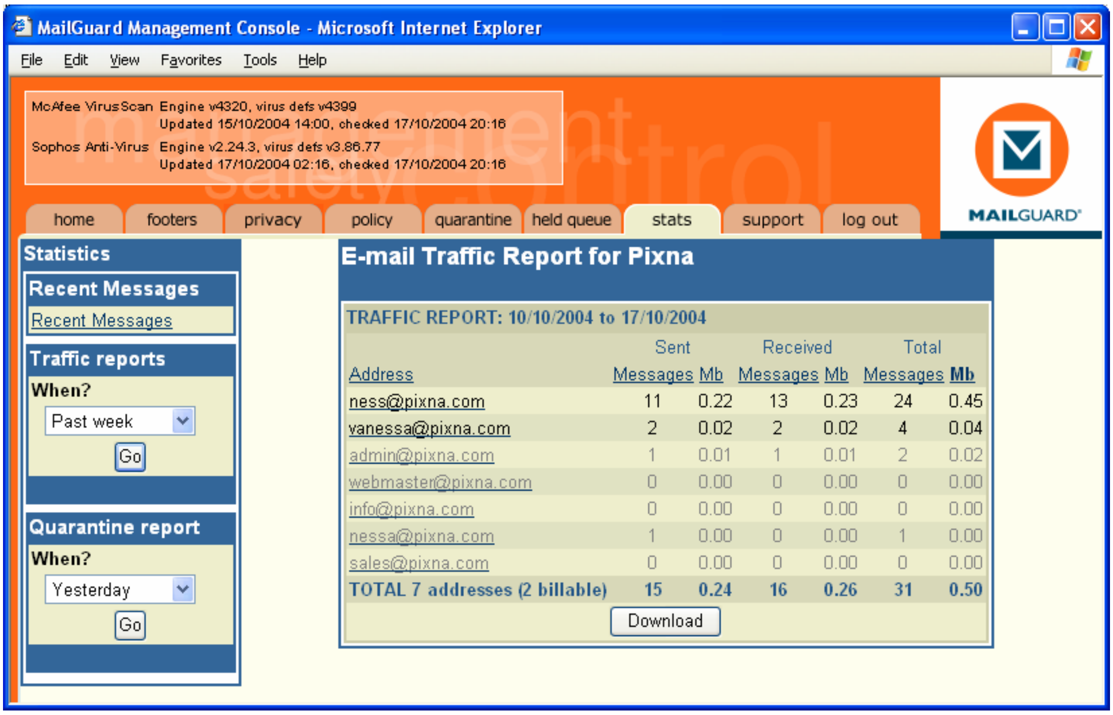
McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 20:03
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 20:03

Recent Messages for Response Design (today only)

Received	From	To	Subject	Transit Time	Size	Attachments
17/10/2004 19:25:33	lynton@crabb.com.au	Elise Rackley	Sorry we missed	5 secs	1.2 KB	
17/10/2004 17:34:06	louise.a@responsedesign.com.au	mark@outerspacedesign.com	Lark designs	13 secs	2.3 MB	LARK CONCEPT 5 Ill9.ai LARK CONCEPT 5 Ill9-1.ai LARK CONCEPT 6 ill9.eps LARK CONCEPT 6 ill9-1.eps LARK CONCEPT 7 ill9.eps LARK CONCEPT 7 ill9-1.eps
17/10/2004	louise.a@responsedesign.com.au	mark@outerspacedesign.com	Lark	36 secs	5.0	LARK CONCEPT

The traffic reports tab allows you to view historical information of your peoples email.

First click on the pull-down list box, and select past week, and then press GO.


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD
Statistics
Recent Messages
Traffic reports
When?
Past week
Go
Quarantine report
When?
Yesterday
Go
Download

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 20:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 20:16

E-mail Traffic Report for Pixna

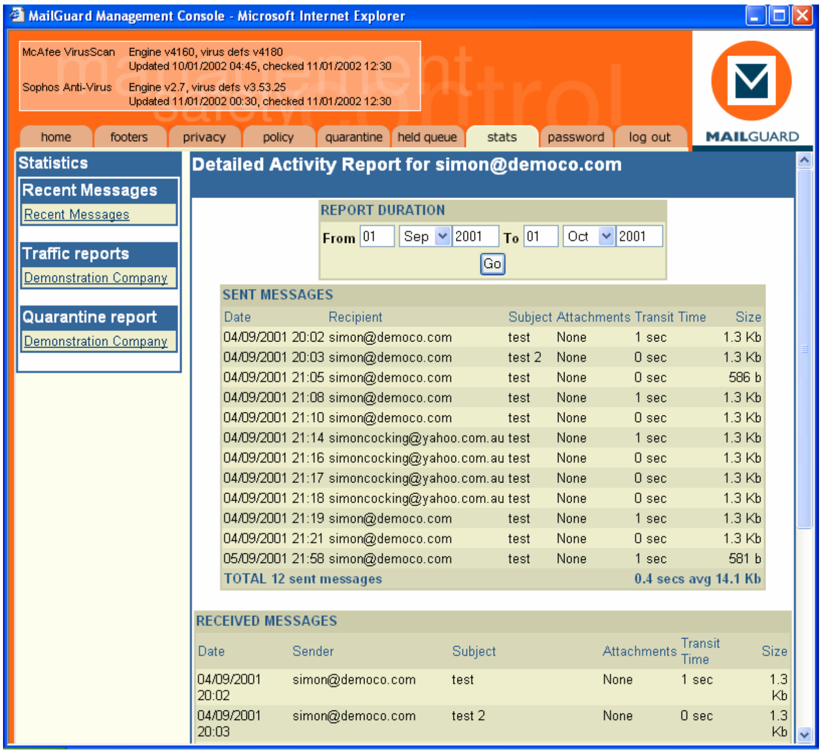
TRAFFIC REPORT: 10/10/2004 to 17/10/2004

	Sent		Received		Total	
Address	Messages	Mb	Messages	Mb	Messages	Mb
ness@pixna.com	11	0.22	13	0.23	24	0.45
vanessa@pixna.com	2	0.02	2	0.02	4	0.04
admin@pixna.com	1	0.01	1	0.01	2	0.02
webmaster@pixna.com	0	0.00	0	0.00	0	0.00
info@pixna.com	0	0.00	0	0.00	0	0.00
nessa@pixna.com	1	0.00	0	0.00	1	0.00
sales@pixna.com	0	0.00	0	0.00	0	0.00
TOTAL 7 addresses (2 billable)	15	0.24	16	0.26	31	0.50

The traffic report screen provides the ability to easily view the users of email within your organisation. This list may be sorted by Sent message, Received message or total megabytes simply by clicking on the appropriate headings.

#

By selecting the individual email address, you may then view the actual “sender, recipient, subject and attachment names” that have contributed towards these statistics.



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 12:30

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 12:30

Detailed Activity Report for simon@democo.com

REPORT DURATION

From 01 Sep 2001 To 01 Oct 2001 Go

SENT MESSAGES

Date	Recipient	Subject	Attachments	Transit Time	Size
04/09/2001 20:02	simon@democo.com	test	None	1 sec	1.3 Kb
04/09/2001 20:03	simon@democo.com	test 2	None	0 sec	1.3 Kb
04/09/2001 21:05	simon@democo.com	test	None	0 sec	586 b
04/09/2001 21:08	simon@democo.com	test	None	1 sec	1.3 Kb
04/09/2001 21:10	simon@democo.com	test	None	0 sec	1.3 Kb
04/09/2001 21:14	simoncocking@yahoo.com.au	test	None	1 sec	1.3 Kb
04/09/2001 21:16	simoncocking@yahoo.com.au	test	None	0 sec	1.3 Kb
04/09/2001 21:17	simoncocking@yahoo.com.au	test	None	0 sec	1.3 Kb
04/09/2001 21:18	simoncocking@yahoo.com.au	test	None	0 sec	1.3 Kb
04/09/2001 21:19	simon@democo.com	test	None	1 sec	1.3 Kb
04/09/2001 21:21	simon@democo.com	test	None	0 sec	1.3 Kb
05/09/2001 21:58	simon@democo.com	test	None	1 sec	581 b
TOTAL 12 sent messages				0.4 secs avg	14.1 Kb

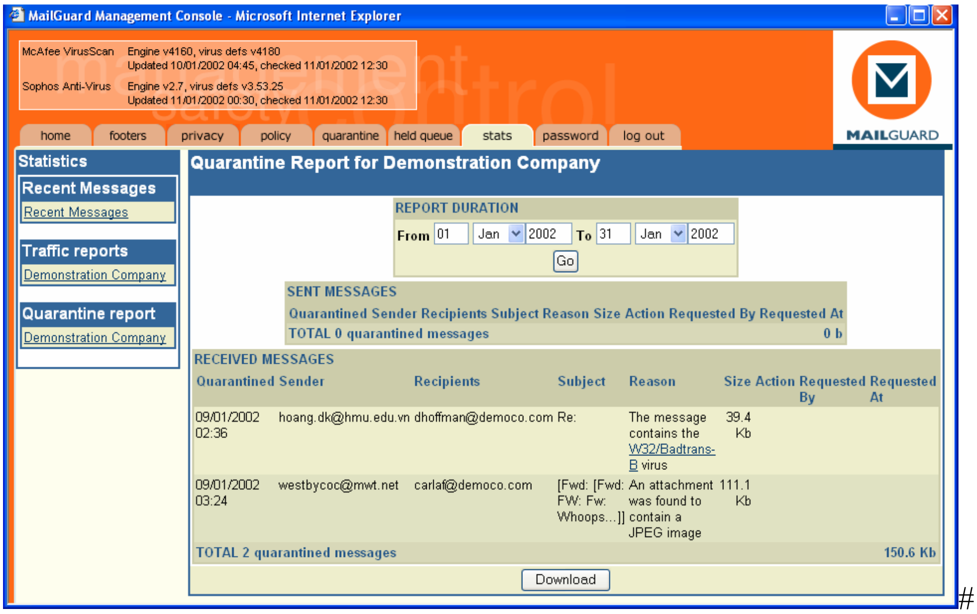
RECEIVED MESSAGES

Date	Sender	Subject	Attachments	Transit Time	Size
04/09/2001 20:02	simon@democo.com	test	None	1 sec	1.3 Kb
04/09/2001 20:03	simon@democo.com	test 2	None	0 sec	1.3 Kb

CleanMail also provides the facility to download statistics to a Microsoft Excel Spreadsheet or “CSV file” by selecting the “Download” button.

3.11.2 Quarantine Report

#



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 12:30

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 12:30

Quarantine Report for Demonstration Company

REPORT DURATION

From 01 Jan 2002 To 31 Jan 2002 Go

SENT MESSAGES

Quarantined	Sender	Recipients	Subject	Reason	Size	Action	Requested By	Requested At
TOTAL 0 quarantined messages					0 b			

RECEIVED MESSAGES

Quarantined	Sender	Recipients	Subject	Reason	Size	Action	Requested By	Requested At
09/01/2002 02:36	hoang.dk@hmu.edu.vn	dhoffman@democo.com	Re:	The message contains the W32/Badtrans-B virus	39.4 Kb			
09/01/2002 03:24	westbycoc@mwt.net	carlaf@democo.com	[Fwd: [Fwd: FW: Fw: Whoops...]]	An attachment was found to contain a JPEG image	111.1 Kb			
TOTAL 2 quarantined messages					150.6 Kb			

#

#

The quarantine report shows messages that have been quarantined over a period of time.

#

#

#

#

3.12 Log Out

The log-out tab allows you to logout from the management console.

4 Setup and Management

CleanMail is designed to be as flexible as possible in the various types of policies and actions that may be configured to meet the needs of your business. We have provided some example policies that are frequently requested for your convenience.

4.1 Setting Policies for Individuals or Domains

#

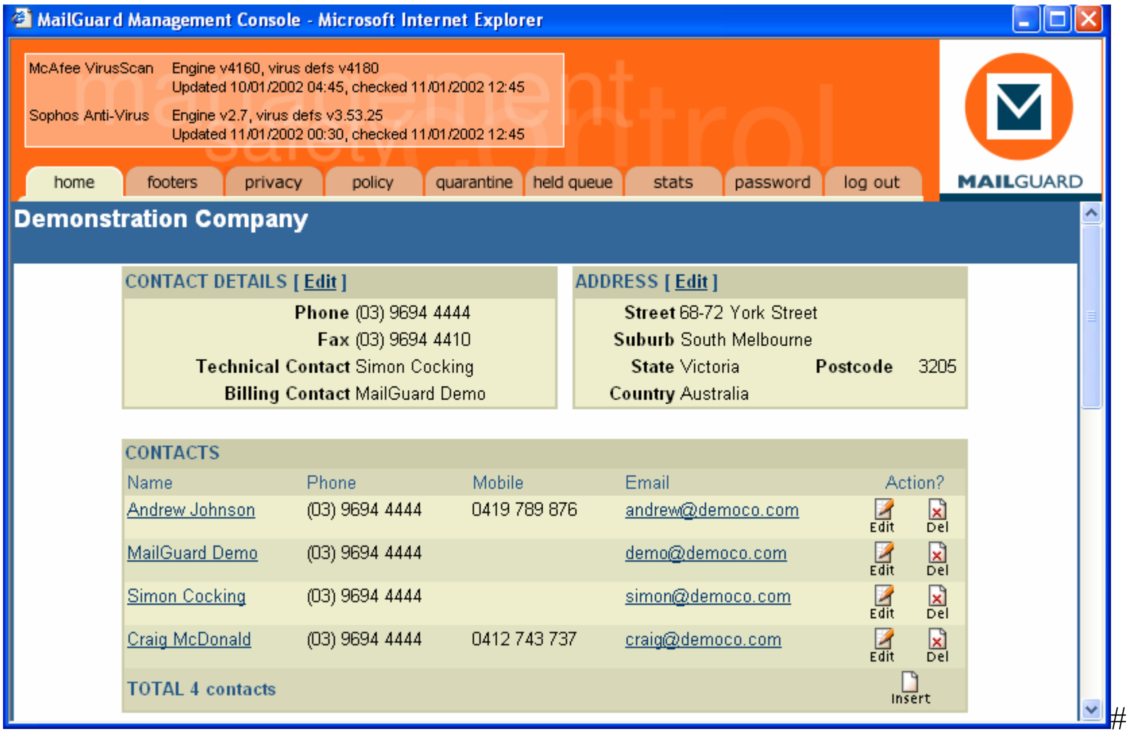
Policies that apply to individual email addresses, or specific domains take precedence over company wide policies, and may be used to set exceptions or extra rules (please be aware that it is possible to override the company-wide AV policy with individual contact rules – this may not be desirable).

(It should always be considered that the policies are always applied top down in the order that they are listed in the CleanMail policy editor).

An example of this, may be you wish to put a rule in for all of your people, saying to block ".exe" files, however – you wish to receive them yourself – you may setup an individual rule under your "contact" from the "HOME" tab that says if the email is of attachment type ".exe" then let it through.

#

#



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 12:45

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 12:45

Demonstration Company

CONTACT DETAILS [Edit]

Phone (03) 9694 4444
Fax (03) 9694 4410
Technical Contact Simon Cocking
Billing Contact MailGuard Demo

ADDRESS [Edit]

Street 68-72 York Street
Suburb South Melbourne
State Victoria **Postcode** 3205
Country Australia

CONTACTS

Name	Phone	Mobile	Email	Action?
Andrew Johnson	(03) 9694 4444	0419 789 876	andrew@democo.com	Edit Del
MailGuard Demo	(03) 9694 4444		demo@democo.com	Edit Del
Simon Cocking	(03) 9694 4444		simon@democo.com	Edit Del
Craig McDonald	(03) 9694 4444	0412 743 737	craig@democo.com	Edit Del
TOTAL 4 contacts				Insert

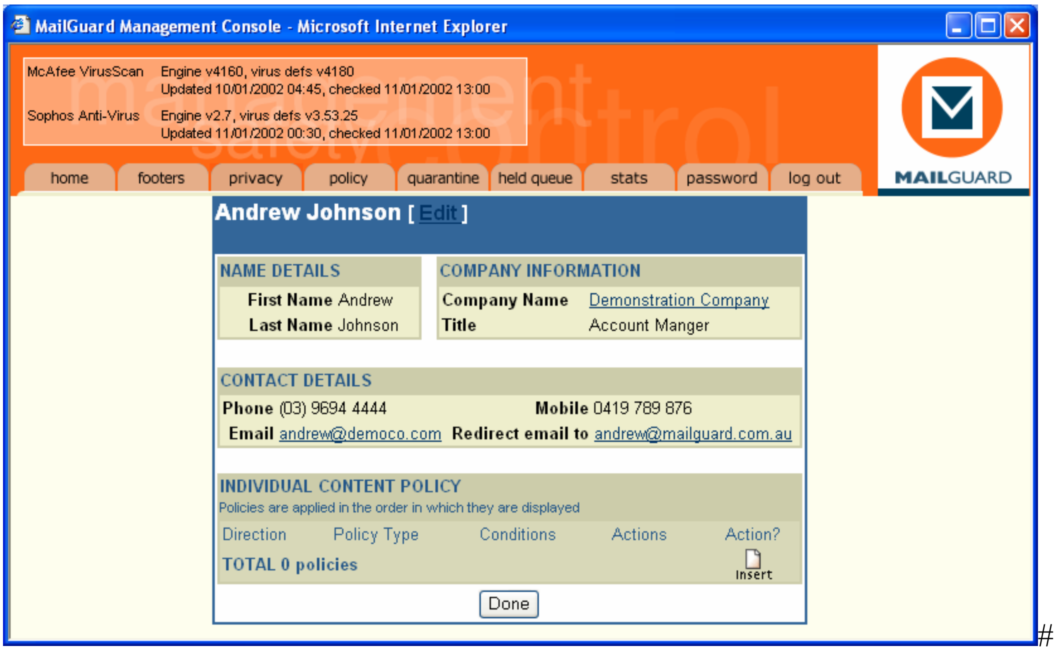
#

#

By selecting the Name of the CONTACT in this page, you may then make changes, and set individual policies for this contact. It should be noted that individual policies may only be configured on people who you have setup as a contact.

#

#



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 11/01/2002 13:00

Sophos Anti-Virus Engine v2.7, virus defs v3.53.25
Updated 11/01/2002 00:30, checked 11/01/2002 13:00

Andrew Johnson [Edit]

NAME DETAILS

First Name Andrew
Last Name Johnson

COMPANY INFORMATION

Company Name Demonstration Company
Title Account Manger

CONTACT DETAILS

Phone (03) 9694 4444 **Mobile** 0419 789 876
Email andrew@democo.com **Redirect email to** andrew@mailguard.com.au

INDIVIDUAL CONTENT POLICY
Policies are applied in the order in which they are displayed

Direction	Policy Type	Conditions	Actions	Action?
TOTAL 0 policies				Insert

#

#

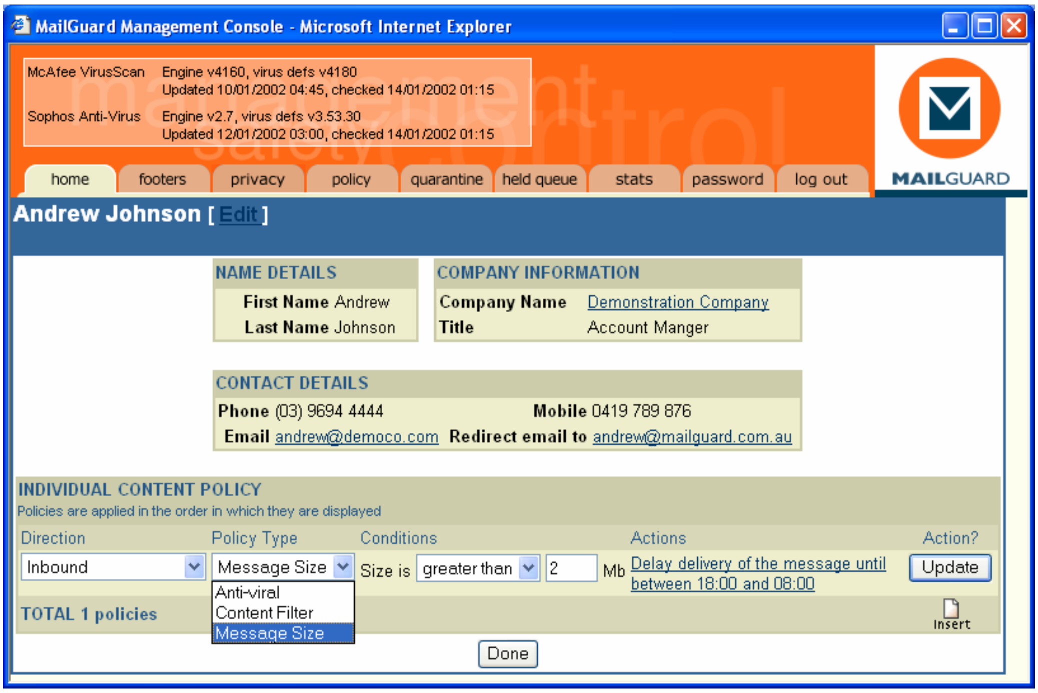
Once the contact has been selected, in this case “Andrew Johnson”, you may then elect to “Edit” their details or proceed to [Insert] a new policy that applies to this contact individually.

#

#

#

After you have selected [Insert] the normal processes for setting up a new policy apply, as detailed in section **3.7 Policy**. All individual polices are also visible (but not editable) from the main policy screen.



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 14/01/2002 01:15

Sophos Anti-Virus Engine v2.7, virus defs v3.53.30
Updated 12/01/2002 03:00, checked 14/01/2002 01:15

Andrew Johnson [Edit]

NAME DETAILS

First Name Andrew
Last Name Johnson

COMPANY INFORMATION

Company Name Demonstration Company
Title Account Manger

CONTACT DETAILS

Phone (03) 9694 4444 **Mobile** 0419 789 876
Email andrew@democo.com **Redirect email to** andrew@mailguard.com.au

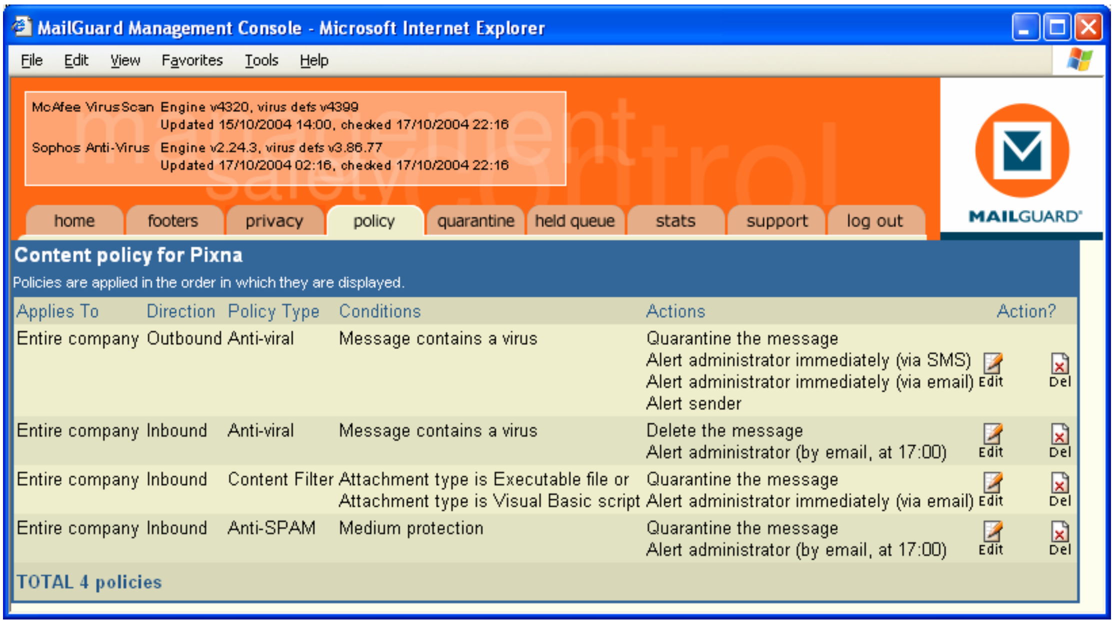
INDIVIDUAL CONTENT POLICY

Policies are applied in the order in which they are displayed

Direction	Policy Type	Conditions	Actions	Action?
Inbound	Message Size Anti-viral Content Filter Message Size	Size is greater than 2 Mb	Delay delivery of the message until between 18:00 and 08:00	Update

TOTAL 1 policies

4.2 Stopping viruses from being sent and received



MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 22:16

Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 22:16

Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Outbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator immediately (via SMS) Alert administrator immediately (via email) Alert sender	Edit Del
Entire company	Inbound	Anti-viral	Message contains a virus	Delete the message Alert administrator (by email, at 17:00)	Edit Del
Entire company	Inbound	Content Filter	Attachment type is Executable file or Attachment type is Visual Basic script	Quarantine the message Alert administrator immediately (via email)	Edit Del
Entire company	Inbound	Anti-SPAM	Medium protection	Quarantine the message Alert administrator (by email, at 17:00)	Edit Del

TOTAL 4 policies

As a basic default policy, there are four policies that are installed into your CleanMail service.

The policy displayed above will perform the following functions:

If a Virus destined for your network is found, CleanMail will delete the virus, and then alert the administrator with a digest email once a day at 5pm.

If a Virus is being sent from within your network to a client or supplier, CleanMail will quarantine the virus, and send a message to the sender (person within your company), and an email and SMS to the administrator for your attention.

If a file of type “Visual Basic Script (.vbs)” or “Executable” is sent to your network, it will be quarantined, and a notification email to you (administrator) for your attention.

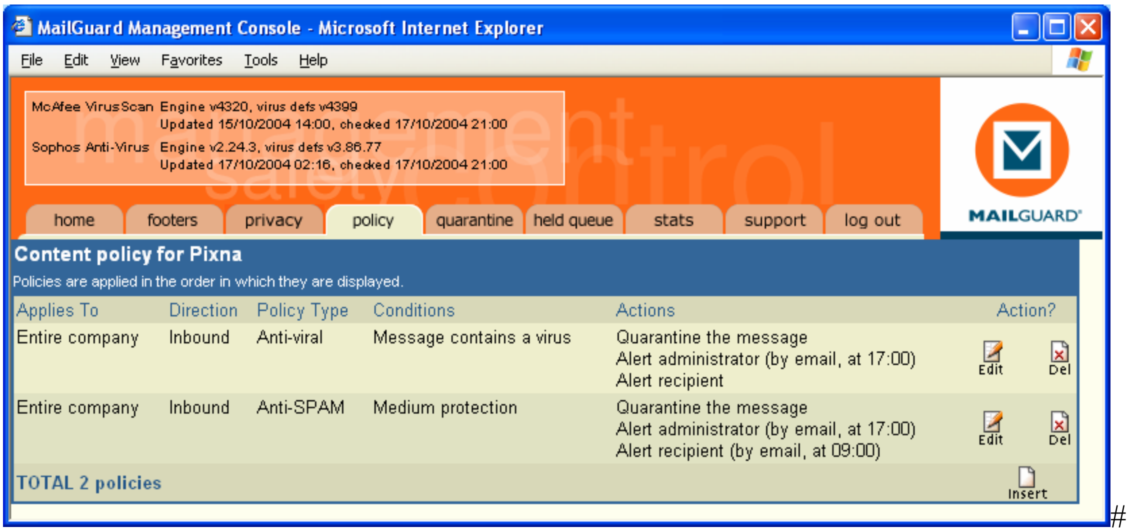
CleanMail’s definition of an “Executable attachment” encompasses any file that CleanMail Guardian may find contains malicious and potentially viral emails. For this reason, we strongly recommend that you do not delete this rule from your policies.

#

#

4.3 STOP SPAM! – SpamGuard®

#



McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 21:00
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 21:00

Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient	Edit Del
Entire company	Inbound	Anti-SPAM	Medium protection	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient (by email, at 09:00)	Edit Del
TOTAL 2 policies					Insert

#

SpamGuard® is CleanMail's sophisticated anti-spam engine that utilises a hybrid of the best of breed spam detection systems available, wrapped into a simple and usable management solution.

Our objective with SpamGuard is to provide a simple system that provides the effectiveness is blocking spam, without the risk of losing real business emails.

SpamGuard takes each message and allocates it a score of "spamminess". This score consists of inputs from one or many of the following sources:

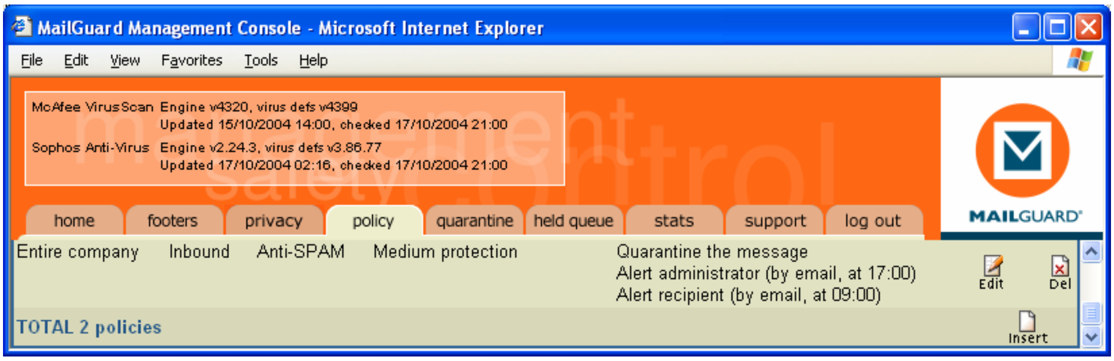
- Spam Assassin Heuristic Inputs and base framework.
- CleanMail weighted spam vocabulary
- Various public blacklists
- Sender Policy Framework
- Bayesian Statistical Input
- Spam fingerprint services (Vipul's Razor etc).

Effective spam protection and productivity gains may be achieved with a varying degree of sophistication and management as required by your business.

4.4 Defining your SPAM Management Profile

Broadly speaking we find that our clients tend to fall into one of the following categories, which will determine the SpamGuard profile that you elect for your business.

DEFAULT: “I want to stop 80% of spam without risking any real messages not coming through, and I don’t want to have to manage anything”.


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MAILGUARD
home footers privacy policy quarantine held queue stats support log out
Edit Del Insert

```
McAfee VirusScan  Engine v4320, virus defs v4399
                  Updated 15/10/2004 14:00, checked 17/10/2004 21:00
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
                  Updated 17/10/2004 02:16, checked 17/10/2004 21:00
```

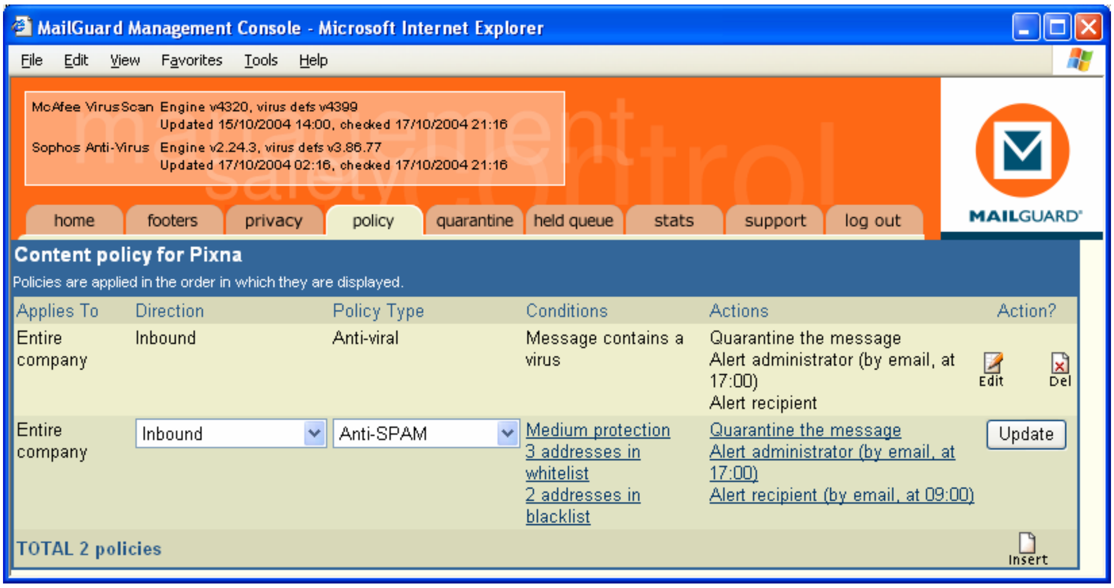
Entire company	Inbound	Anti-SPAM	Medium protection	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient (by email, at 09:00)	Edit Del

TOTAL 2 policies

Key configuration items:

- Digest to end user
- Digest to admin
- Lowest management level required.

ACTIVE: “I want to stop as much spam as possible with minimal risk of blocking real messages, but I am happy to manage white/black lists and release messages as required”.


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MAILGUARD
home footers privacy policy quarantine held queue stats support log out
Insert

```
McAfee VirusScan  Engine v4320, virus defs v4399
                  Updated 15/10/2004 14:00, checked 17/10/2004 21:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
                  Updated 17/10/2004 02:16, checked 17/10/2004 21:16
```

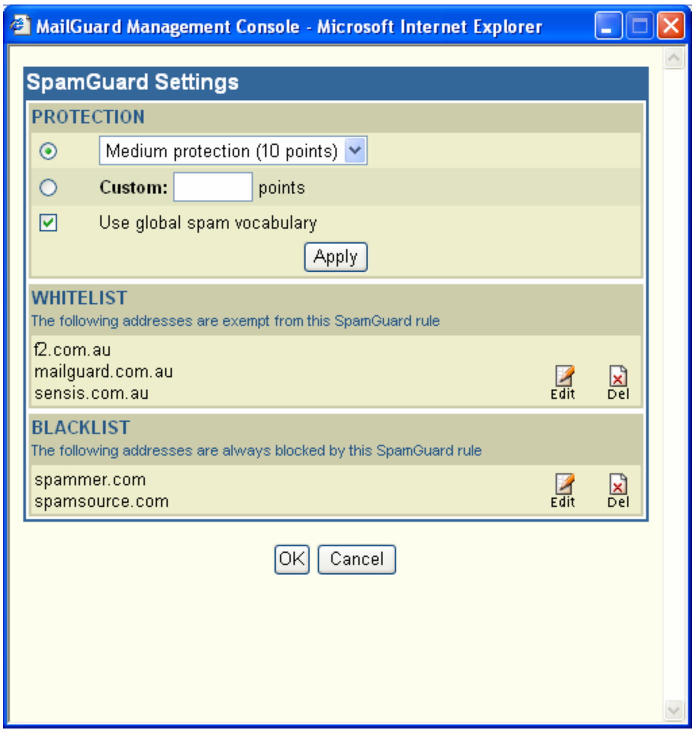
Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient	Edit Del
Entire company	Inbound	Anti-SPAM	Medium protection 3 addresses in whitelist 2 addresses in blacklist	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient (by email, at 09:00)	Update

TOTAL 2 policies

The Whitelists and Blacklists may be accessed by clicking on the Conditions link “Medium Protection”.



SpamGuard Settings

PROTECTION

● Medium protection (10 points)

○ Custom: points

☑ Use global spam vocabulary

Apply

WHITELIST

The following addresses are exempt from this SpamGuard rule

f2.com.au
mailguard.com.au
sensis.com.au

Edit Del

BLACKLIST

The following addresses are always blocked by this SpamGuard rule

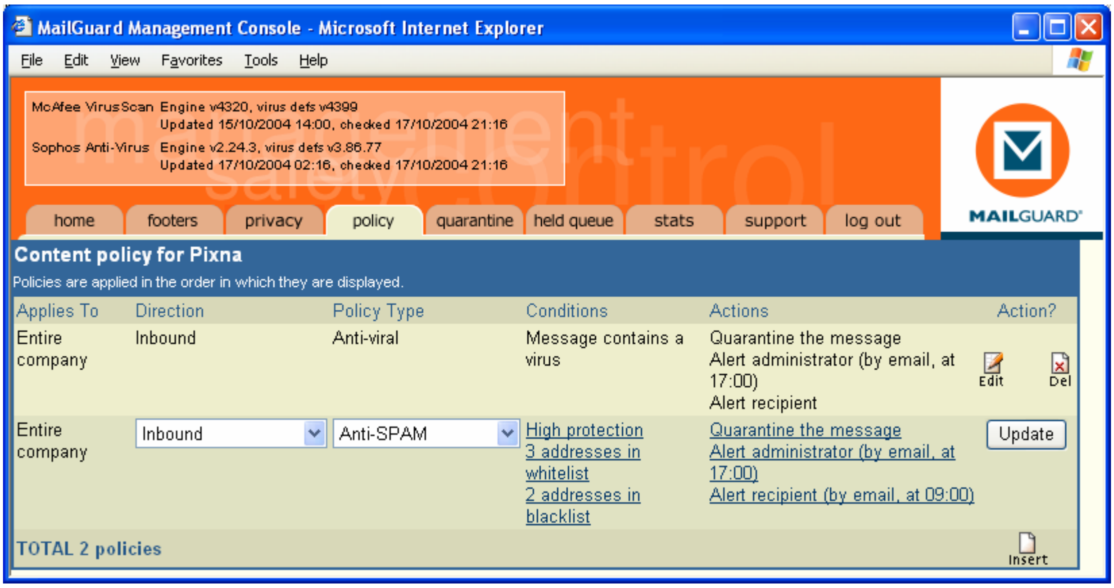
spammer.com
spamsource.com

Edit Del

Key configuration items:

- Administrator managed White & Blacklists
- Digest to admin
- Digest to Recipient

TOTAL CONTROL: “I wish to stop all spam. I am happy to use CleanMail’s SpamGuard, whitelist, blacklists and content filtering policies to tailor my message handling to the point of perfection”.


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 21:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 21:16

Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient	Edit Del
Entire company	Inbound	Anti-SPAM	High protection 3 addresses in whitelist 2 addresses in blacklist	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient (by email, at 09:00)	Update
TOTAL 2 policies					Insert

#

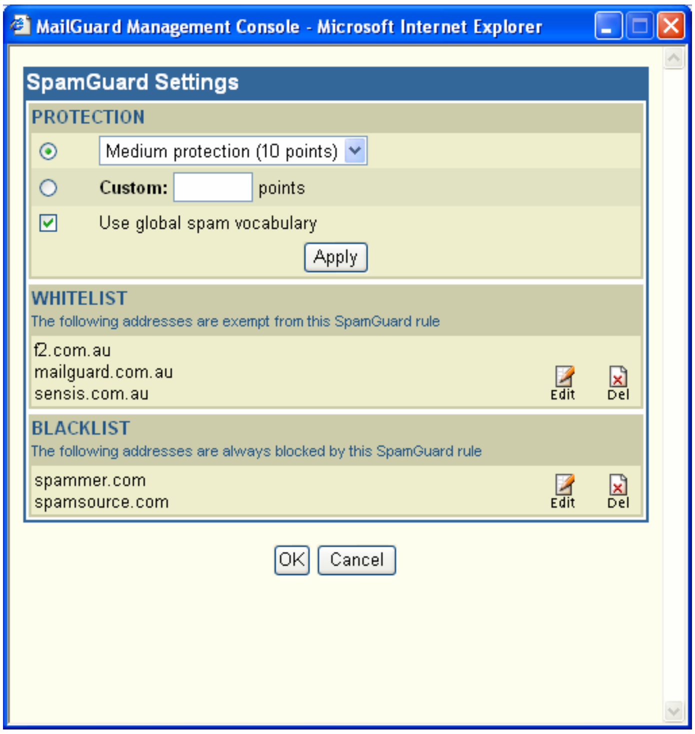
4.5 *SpamGuard Management*

4.5.1 I wish to allow all mail from a particular user or domain

#

Occasionally, as you reduce the tolerance of your SpamGuard setting you will find that some legitimate emails that may have many spam characteristics may be incorrectly stopped by CleanMail. This is known as a false positive.

If you wish to avoid these items being incorrectly classified as spam, you may add them to the SpamGuard whitelist. This whitelist may be accessed by selecting the “Conditions” entry on your Anti-spam rule



MailGuard Management Console - Microsoft Internet Explorer

SpamGuard Settings

PROTECTION

● Medium protection (10 points)

○ **Custom:** points

☑ Use global spam vocabulary

Apply

WHITELIST

The following addresses are exempt from this SpamGuard rule

f2.com.au
mailguard.com.au
sensis.com.au

Edit Del

BLACKLIST

The following addresses are always blocked by this SpamGuard rule

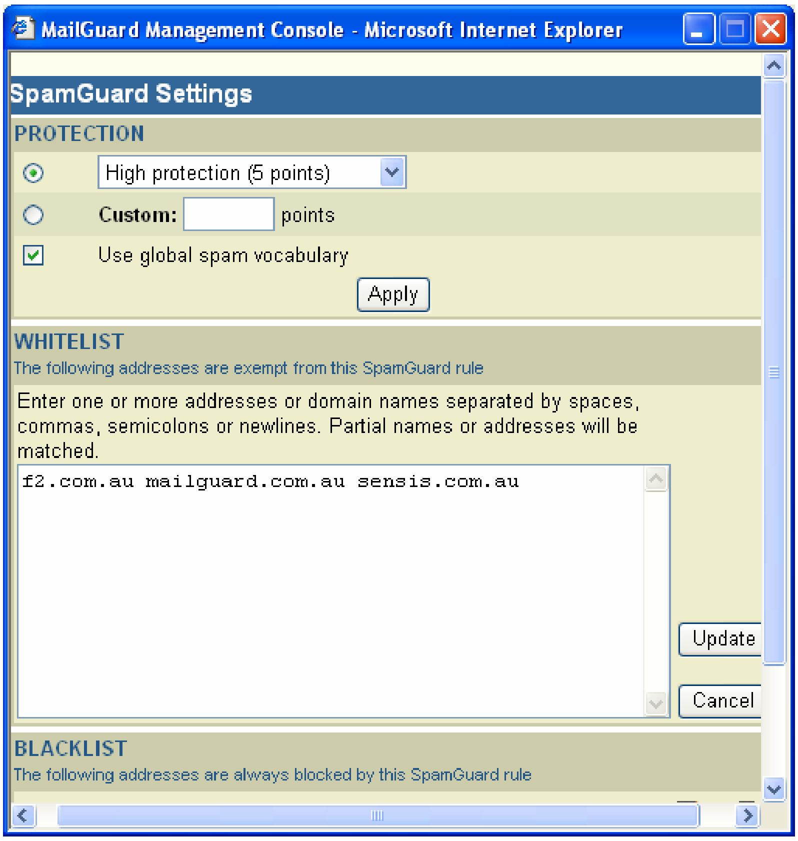
spammer.com
spamsource.com

Edit Del

OK Cancel

You may select the [Edit] button that allows you to add/maintain your white and black lists.

#



SpamGuard Settings

PROTECTION

● High protection (5 points)

○ Custom: points

☑ Use global spam vocabulary

WHITELIST

The following addresses are exempt from this SpamGuard rule

Enter one or more addresses or domain names separated by spaces, commas, semicolons or newlines. Partial names or addresses will be matched.

```
f2.com.au mailguard.com.au sensis.com.au
```

BLACKLIST

The following addresses are always blocked by this SpamGuard rule

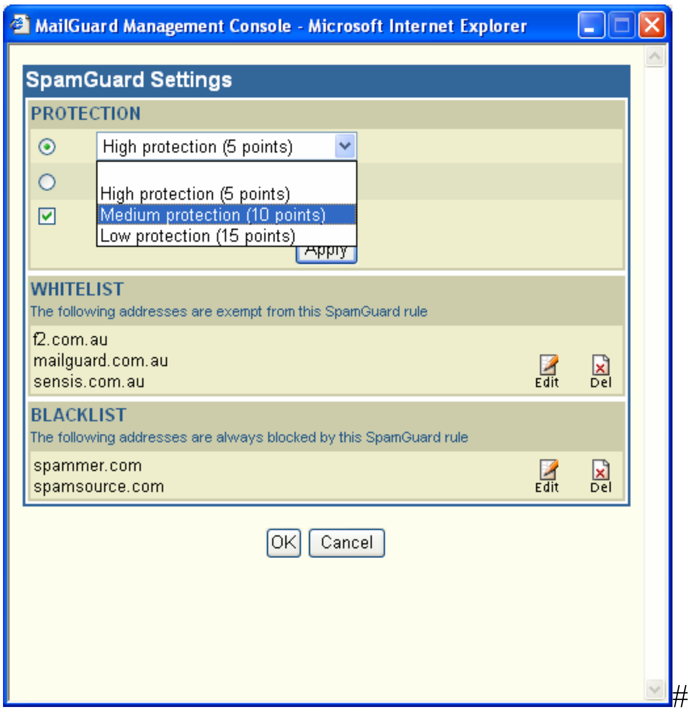
Individual email addresses, or domains may be entered into the whitelist space separated by spaces.

Black lists may be managed in the same way.

#

4.5.2 We are still receiving too much spam – how can I tune SpamGuard?

The default SpamGuard tolerance setting is 10 points (Medium). This setting may be tuned to a lower tolerance to spam (less than 10 points) as can be seen in the screen below:



MailGuard Management Console - Microsoft Internet Explorer

SpamGuard Settings

PROTECTION

● High protection (5 points)

○

☑

High protection (5 points)
Medium protection (10 points)
Low protection (15 points)

WHITELIST

The following addresses are exempt from this SpamGuard rule

f2.com.au
mailguard.com.au
sensis.com.au

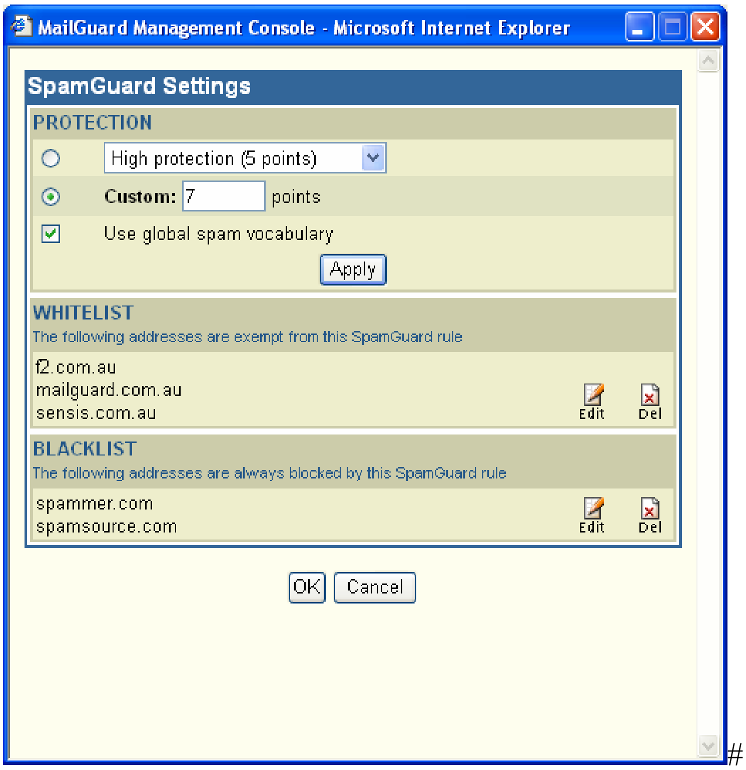
BLACKLIST

The following addresses are always blocked by this SpamGuard rule

spammer.com
spamsource.com

#

Alternately, a custom setting may also be entered.



MailGuard Management Console - Microsoft Internet Explorer

SpamGuard Settings

PROTECTION

○ High protection (5 points)

● Custom: 7 points

☑ Use global spam vocabulary

WHITELIST

The following addresses are exempt from this SpamGuard rule

f2.com.au
mailguard.com.au
sensis.com.au

BLACKLIST

The following addresses are always blocked by this SpamGuard rule

spammer.com
spamsource.com

#

#

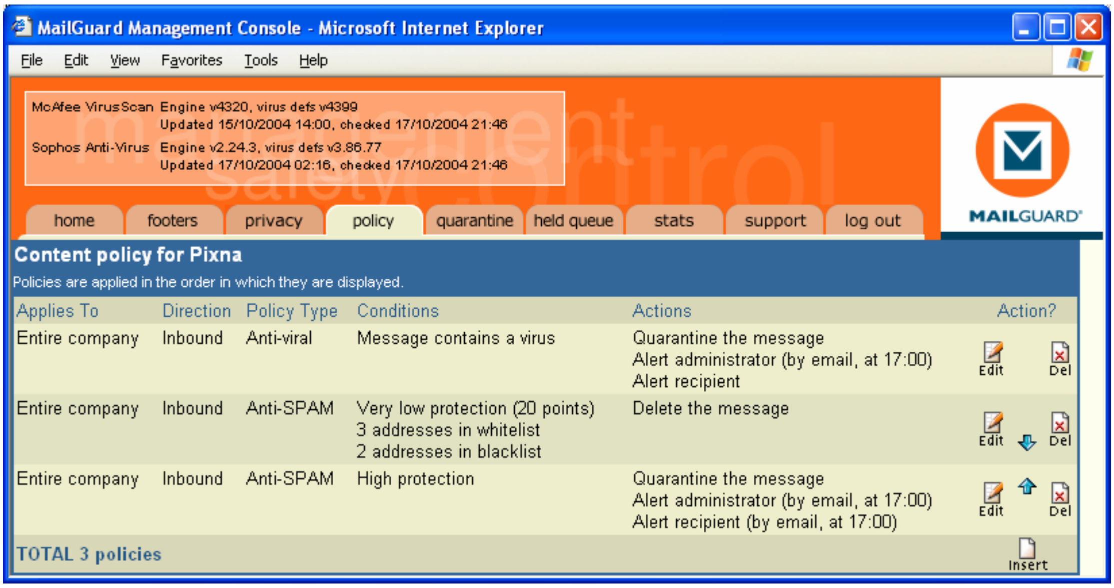
After reducing your SpamGuard tolerance score, we recommend that you actively monitor your quarantine to make sure that you are not stopping any false positives.
#

4.5.3 I am receiving too many items in my quarantine/spam digest!

If a large volume of spam is being received by your business and stopped by CleanMail, the amount of items in your CleanMail digest and quarantine may become overwhelming.

In this case we recommend that our clients simplify the management of their spam by deleting rather than quarantining those emails that are blatantly spam.

We achieve this by entering a cascading anti-spam rule as follows:



McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 21:46
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 21:46

Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Inbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient	Edit Del
Entire company	Inbound	Anti-SPAM	Very low protection (20 points) 3 addresses in whitelist 2 addresses in blacklist	Delete the message	Edit ↓ Del
Entire company	Inbound	Anti-SPAM	High protection	Quarantine the message Alert administrator (by email, at 17:00) Alert recipient (by email, at 17:00)	Edit ↑ Del
TOTAL 3 policies					Insert

#
All emails that are blatantly spam are deleted by the top rule as they would rate greater than 20 points.

Any items that are likely to be spam (between 5 and 20 points) are then quarantined as per normal, and sent as a digest email to the administrator at 17:00.
#

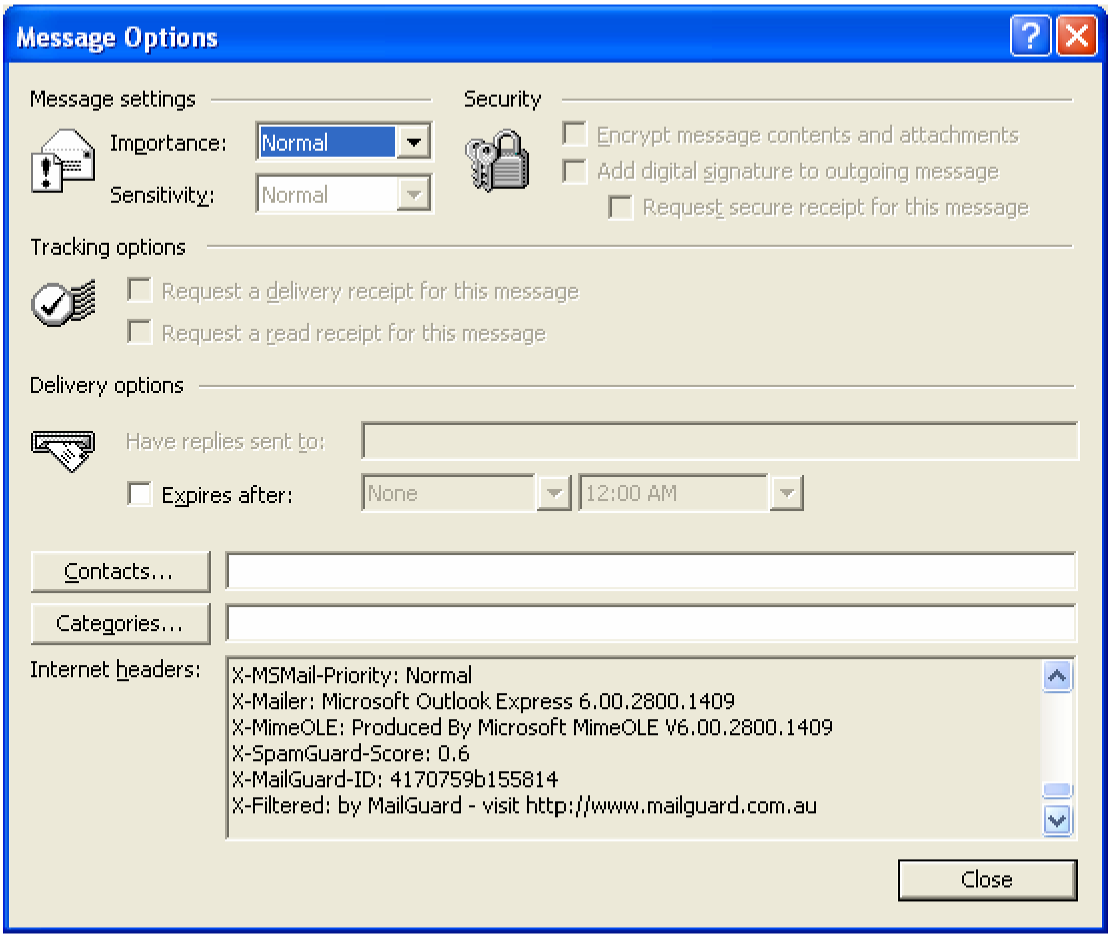
#

#

4.5.4 How do I view the spam score on a message?

Occasionally a spam message will score so low that it is not picked up by SpamGuard rules, and you may wish to check how it scored.

You can do this by viewing the headers of the email. In Outlook this may be done by opening the message and then selecting View and then “Options”.



Importance: Normal

Sensitivity: Normal

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request secure receipt for this message

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Have replies sent to:

□ Expires after: None 12:00 AM

Internet headers:

```
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1409
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1409
X-SpamGuard-Score: 0.6
X-MailGuard-ID: 4170759b155814
X-Filtered: by MailGuard - visit http://www.mailguard.com.au
```

The header: X-SpamGuard-Score: 0.6 shows that this particular message rated as 0.6.

This is valuable information in working with CleanMail to optimize your spam protection.

#

#

#

#

#

#

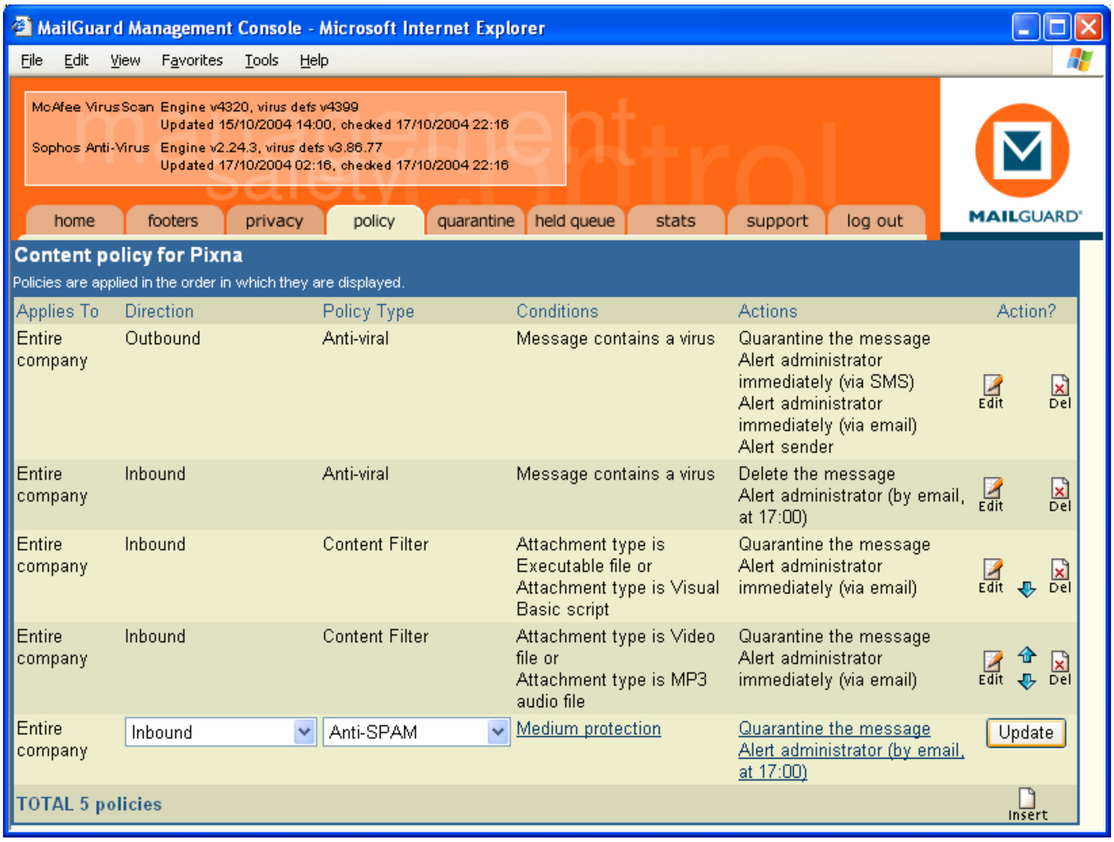
#

#

#

#

4.6 *Blocking certain file types – "Movie and MP3 etc"*


MailGuard Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
home footers privacy policy quarantine held queue stats support log out
MAILGUARD

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 22:16
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 22:16

Content policy for Pixna

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Entire company	Outbound	Anti-viral	Message contains a virus	Quarantine the message Alert administrator immediately (via SMS) Alert administrator immediately (via email) Alert sender	Edit Del
Entire company	Inbound	Anti-viral	Message contains a virus	Delete the message Alert administrator (by email, at 17:00)	Edit Del
Entire company	Inbound	Content Filter	Attachment type is Executable file or Attachment type is Visual Basic script	Quarantine the message Alert administrator immediately (via email)	Edit ⇩ Del
Entire company	Inbound	Content Filter	Attachment type is Video file or Attachment type is MP3 audio file	Quarantine the message Alert administrator immediately (via email)	Edit ⇧ ⇩ Del
Entire company	Inbound	Anti-SPAM	Medium protection	Quarantine the message Alert administrator (by email, at 17:00)	Update
TOTAL 5 policies					Insert

Content Filters allow you to block email by attachment type, key word, sender address, recipient addresses or filename. Essentially the content filter looks through every word in your email and attachment and decides whether it meets the criteria set.

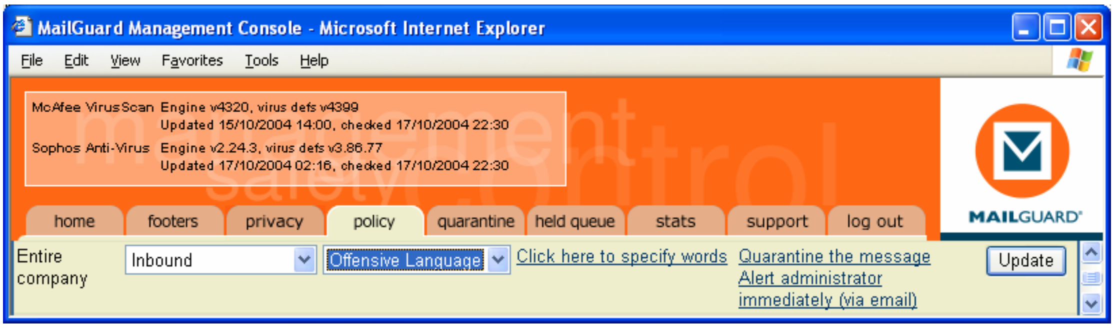
Attachment type content filtering is particularly useful to control and monitor the transit of certain types of email entering and leaving your business.

The rules above perform the following functions:

Applying to the entire company, when an email is sent to someone in the organisation and it contains a video file or music file, it will be quarantined, with an alert sent to the administrator.

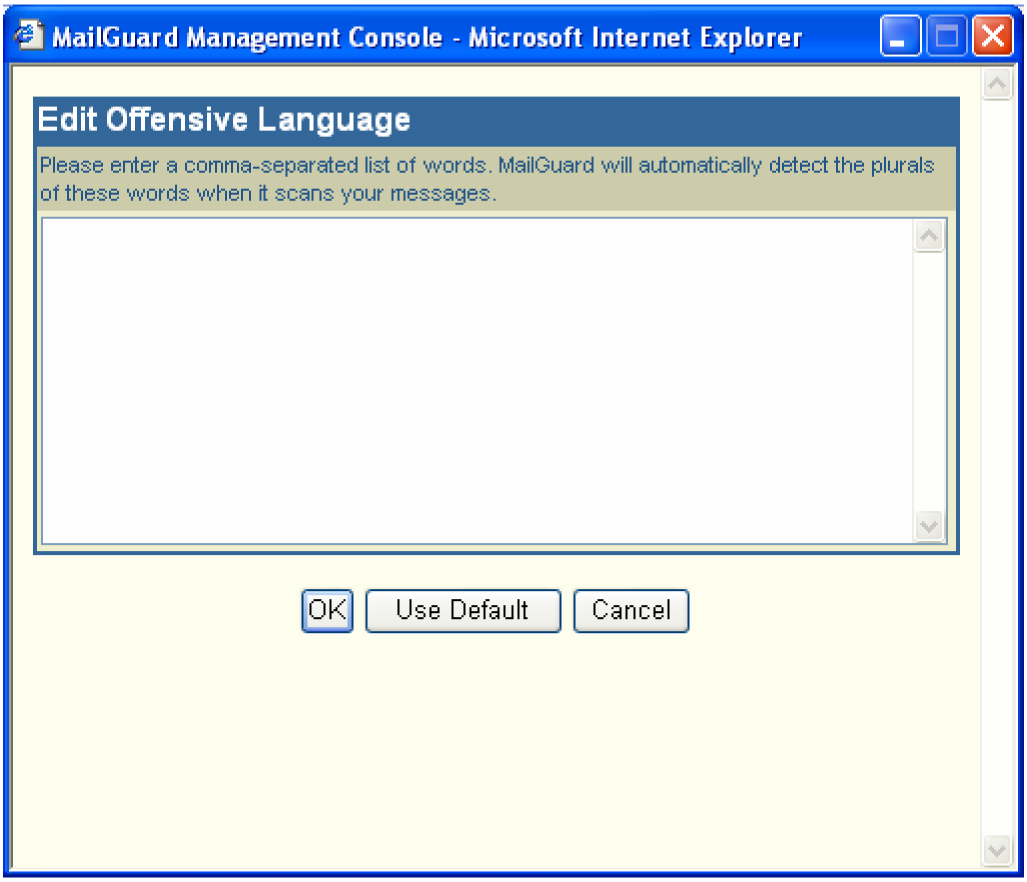
4.7 *Managing offensive or inappropriate emails*

By applying an “Offensive Language” policy, you are able to have emails that contain particular key words, quarantined with a copy sent only to the administrator. After viewing the email, you may then elect as to whether to allow the email to the recipient or otherwise.


MailGuard Management Console - Microsoft Internet Explorer

McAfee VirusScan Engine v4320, virus defs v4399
Updated 15/10/2004 14:00, checked 17/10/2004 22:30
Sophos Anti-Virus Engine v2.24.3, virus defs v3.86.77
Updated 17/10/2004 02:16, checked 17/10/2004 22:30

Entire company | Inbound | Offensive Language | Click here to specify words | Quarantine the message Alert administrator immediately (via email)


MailGuard Management Console - Microsoft Internet Explorer

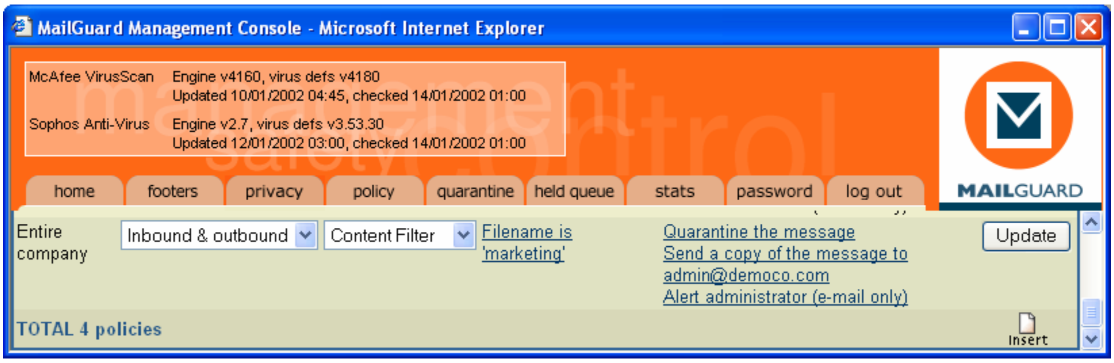
Edit Offensive Language

Please enter a comma-separated list of words. MailGuard will automatically detect the plurals of these words when it scans your messages.

4.8 *Stopping confidential documents leaving via email*

Many companies at one stage or another are faced with the prospect of strategic people leaving your organisation. Today, email makes it easier than ever for these people to send themselves *(to a home email address),* confidential documents such a projections, marketing plans etc.

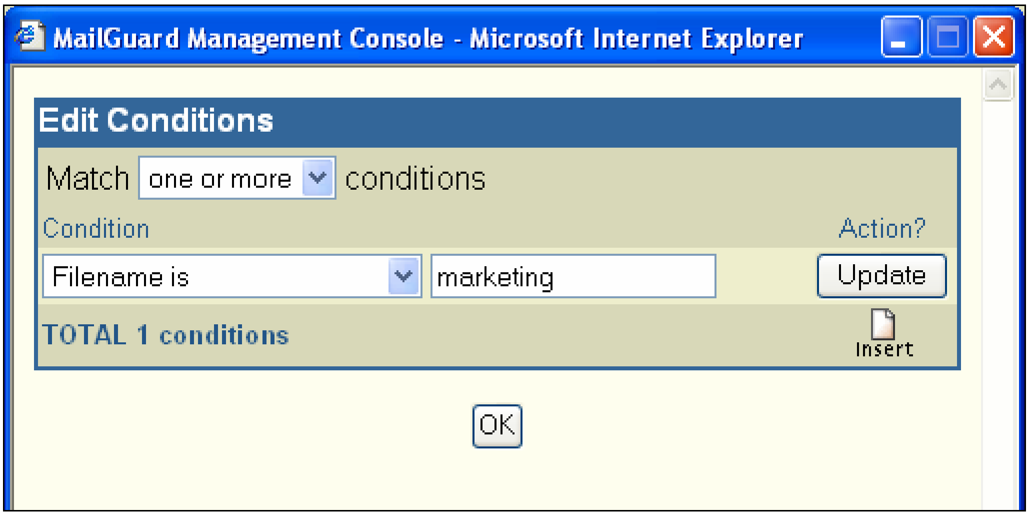
With CleanMail, it is possible to select particular filenames or wildcard filenames ie. **"Marketing*"** or **"Budget*"** that will trigger a policy when an attempt is made to send confidential documents outside your organisation.



McAfee VirusScan Engine v4160, virus defs v4180
Updated 10/01/2002 04:45, checked 14/01/2002 01:00
Sophos Anti-Virus Engine v2.7, virus defs v3.53.30
Updated 12/01/2002 03:00, checked 14/01/2002 01:00

Entire company	Inbound & outbound	Content Filter	Filename is 'marketing'	Quarantine the message Send a copy of the message to admin@democo.com Alert administrator (e-mail only)

TOTAL 4 policies



Edit Conditions

Match one or more conditions

Condition		Action?
Filename is	marketing	

TOTAL 1 conditions

With this policy in place, any email that has a file attached to it with the filename **"marketing"** at the start of it – will be quarantined, with a copy sent to the administrator for your perusal. From quarantine, you may then release the email to the recipient, delete it or forward it to another email address.

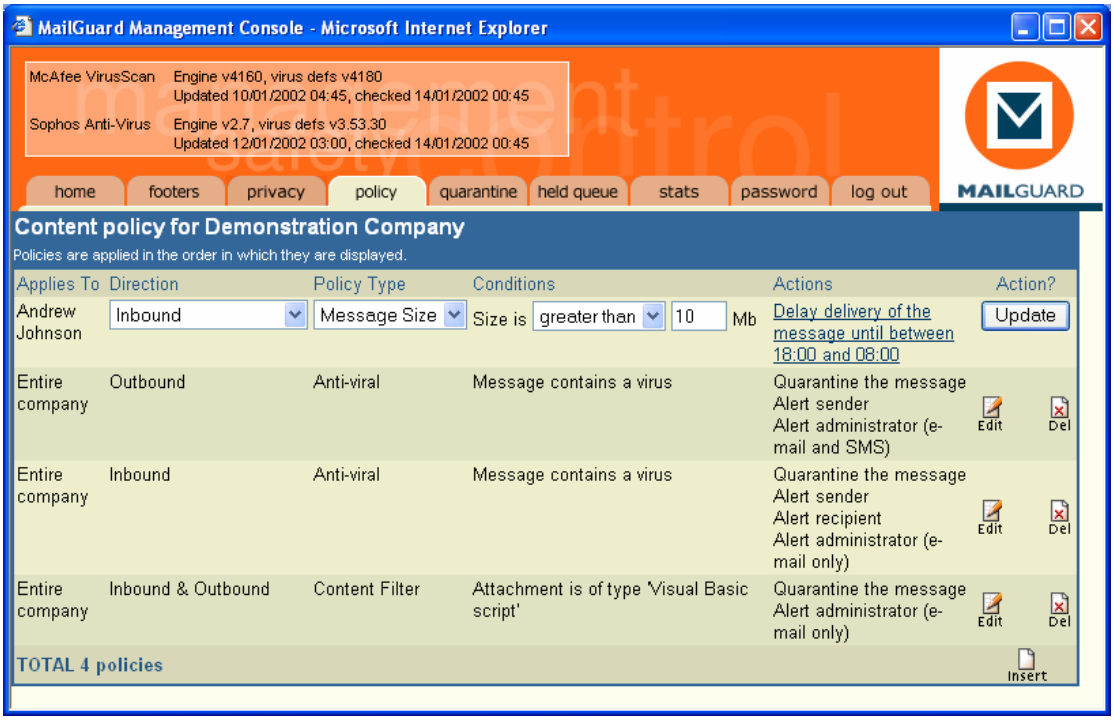
4.9 *Stopping/Delaying large files before they get to you*

CleanMail provides a facility whereby we can create polices based on the size of the email. If an email is greater than, equal to, or less than specific sizes CleanMail can perform the normal actions, and alerts of any CleanMail policy.

This function is particularly useful for circumstances where your **Internet connection bandwidth is critical to the performance of your business**.

The policy that we have installed below allows all emails that are larger than 5mb to be delivered after 8pm. We have also elected to notify the recipient that they have received email, however it will be delivered after hours.

This allows the recipient to contact the administrator to override the hold on the email if it is urgent.



MailGuard Management Console - Microsoft Internet Explorer

McAfee VirusScan	Engine v4160, virus defs v4180 Updated 10/01/2002 04:45, checked 14/01/2002 00:45
Sophos Anti-Virus	Engine v2.7, virus defs v3.53.30 Updated 12/01/2002 03:00, checked 14/01/2002 00:45

Content policy for Demonstration Company

Policies are applied in the order in which they are displayed.

Applies To	Direction	Policy Type	Conditions	Actions	Action?
Andrew Johnson	Inbound	Message Size	Size is greater than 10 Mb	Delay delivery of the message until between 18:00 and 08:00	Update
Entire company	Outbound	Anti-viral	Message contains a virus	Quarantine the message Alert sender Alert administrator (e-mail and SMS)	Edit Del
Entire company	Inbound	Anti-viral	Message contains a virus	Quarantine the message Alert sender Alert recipient Alert administrator (e-mail only)	Edit Del
Entire company	Inbound & Outbound	Content Filter	Attachment is of type 'Visual Basic script'	Quarantine the message Alert administrator (e-mail only)	Edit Del

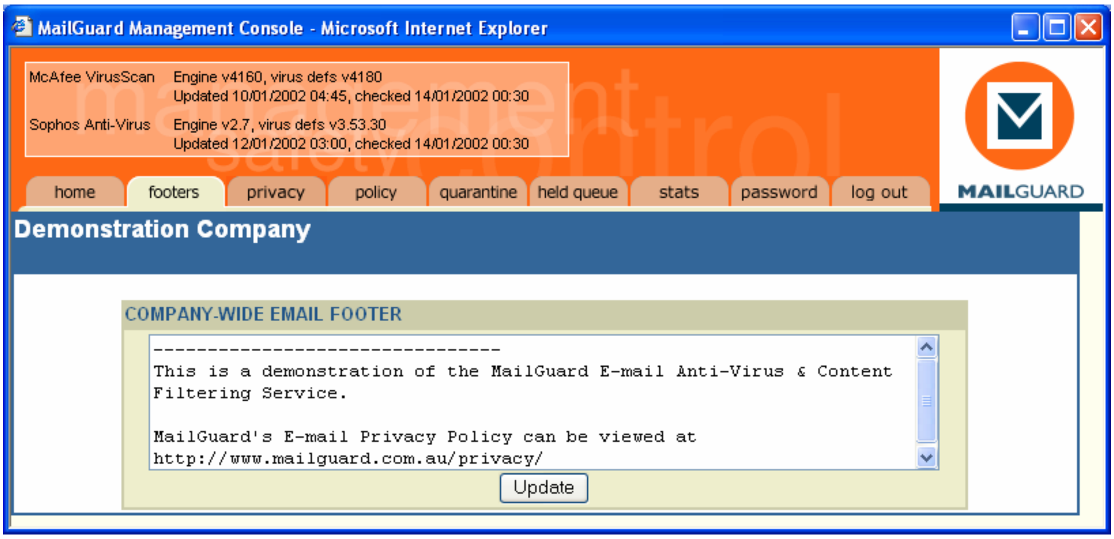
TOTAL 4 policies

#

4.10 *Setting up Company Wide Footers*

Company-wide footers are often useful for disclaimer messages and may be configured in the “footer” tab.

The footers area of the management console allows a”Company-Wide” footer for all organisations that are within your company. This will apply to every domain that is being managed by your management console, and will be automatically attached to every outgoing email.



```
McAfee VirusScan    Engine v4160, virus defs v4180
                    Updated 10/01/2002 04:45, checked 14/01/2002 00:30

Sophos Anti-Virus   Engine v2.7, virus defs v3.53.30
                    Updated 12/01/2002 03:00, checked 14/01/2002 00:30
```

Demonstration Company

COMPANY-WIDE EMAIL FOOTER

```
--------------------------------
This is a demonstration of the MailGuard E-mail Anti-Virus & Content
Filtering Service.

MailGuard's E-mail Privacy Policy can be viewed at
http://www.mailguard.com.au/privacy/
```

#

#

#

5 Further Help on CleanMail

If you require further help with CleanMail, please do not hesitate to contact us:

Support ***business.techsupport@pacific.net.au*** **Phone:** 13 36 39