

Table of Contents

About this Guide.....	2
Introduction.....	3
Features.....	3
Login.....	4
Navigation.....	4
Welcome.....	5
Protection Levels.....	5
Off.....	5
Low.....	5
Medium.....	5
High.....	5
Cache contents.....	5
Stats.....	6
White/Black List.....	6
Settings.....	6
Email Addresses.....	6
Login Credentials.....	6
Miscellaneous Settings.....	6
Admin.....	7
Users.....	7
Lookup User.....	7
Add New Email Address/Alias.....	7
Link E-mail Address/Alias.....	8
Delete E-mail Address/Alias and Delete Users.....	8
Domains.....	8
Filter Settings.....	9
Virus Scanning.....	9
Spam Filtering.....	9
Attachment Type Filtering.....	10
Bad Header Filtering.....	10
Domain Specific Filters.....	10
Non-spam item caching.....	10
SMTP IPs	10
Add Administrator.....	10
Cache Contents.....	11
Email View.....	11
Releasing Quarantined Email.....	12
Using the Service – MX Records.....	12
Appendix A – List of filtered attachments.....	13

About this Guide

This guide is intended to be a brief introduction to Mailguard, to explain how Mailguard works and how you can configure it for use with your domain.

Introduction

Mailguard is an e-mail filtering and anti virus solution built using the powerful, tried and tested open source tools used by companies worldwide.

It provides you with an easy to use web interface to customise what actions to take when potentially unsolicited email is received as well as the ability to customise the strength of the protection to suit your needs.

Features

- Per user customisable filtering of unsolicited email
- Per domain customisable filtering of unsolicited email
- Built in virus scanning
- Attachment type filtering
- Labelling of unsolicited email
- Quarantining of dangerous and unsolicited emails

Login

When you receive your login details you should open a web browser to the following URL:

<https://mailguard.vorari.net/>

This will take you to the login screen pictured below, from here enter the user name and password provided and you will be logged into the control panel for your user and placed on the welcome screen.



Navigation

Along the left hand side of the control panel is the navigation bar, along with a summary of the number of emails stored in Mailguards cache and the name of the user you're currently logged in as.

Unconfirmed Non-spam:	1
Suspected Spam:	2
Virus/Malware:	1

Username:
scott@vorari.net

Welcome

Protection Levels



Off

The 'off' level offers no protection at all. All scanning is disabled, so the filter is effectively transparent, letting everything through

Low

At the 'low' protection setting, only virus scanning is performed

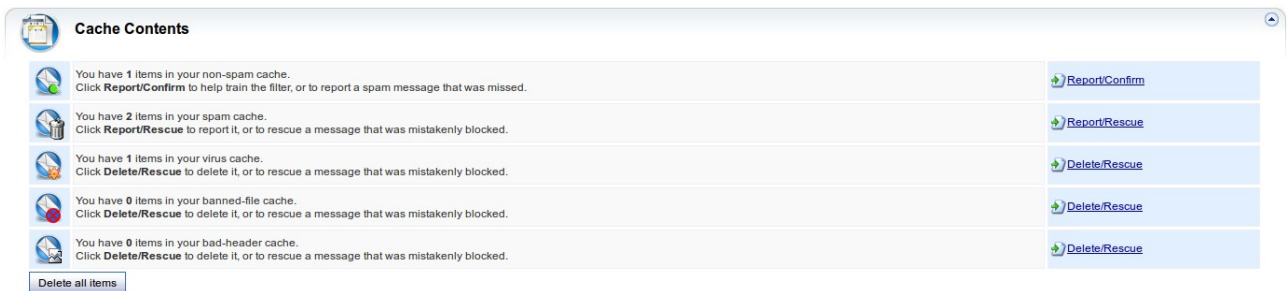
Medium

The 'medium' protection setting adds spam scoring headers to the mail when it scores 5.0 or higher, but does not quarantine or discard it. Banned file attachments and mail with invalid headers are passed through

High

The 'high' protection setting adds spam scoring headers to the mail when it scores 1.0 or higher, and quarantines spam that scores 5.0 or higher, along with viruses, banned file attachments, and mail with invalid headers

Cache contents



The cache contents shows a summary of emails that have passed through the system and haven't been marked to indicate if they were legitimate or unsolicited emails. From the links on the right of the screen, you're taken to a listing of emails in the cache for that category.

Using the cache contents you're able to train the spam filter so it's able to better identify which emails are valid and which aren't, you can also release emails that have been quarantined and see why emails have been marked as spam. See the section Cache Contents for more details.

Stats

The stats section of Mailguard provides you with various statistics providing you with counts and averages amongst other values to show how many emails have been filtered along with why they were filtered.

White/Black List

This section allows you to add email addresses to the filters white or black list, adding email addresses to the white list will remove 100 points from their spam score, conversely adding an email address to the blacklist adds 100 points to it's spam score.

Settings

Email Addresses

The settings section is where you control your preferences for the control panel. At the top is a list of email addresses assigned to the account you're logged in as. Below that is where you're able to link other email addresses belonging to yourself to this account.

The screenshot shows two panels. The top panel, titled 'E-mail Addresses', contains a table with two columns: 'Addresses' and 'Actions'. The 'Addresses' column lists 'scott@vorari.net'. The 'Actions' column contains a blue 'Edit Settings' link and the text 'Primary Address'. The bottom panel, titled 'Add Address', has a 'Username:' field with 'scott@vorari.net' and a 'Password:' field with '*****'. Below these fields is a button labeled 'Add E-Mail Address'.

To link another address to your account it needs to exist on the system with a user name and password. If you enter the user name and password into the provided text boxes the address will be linked to the account you're logged in as, *doing this will prevent you from logging in as that account as it will be permanently linked to this account. To revert this an administrator will need to remove and re-add the email address.*

The Edit Settings link next to the email address is where you are able to edit the email filtering options and anti virus protection for the email address. See the section Filter Settings for details.

Login Credentials

The login credentials is simply where you change your login password.

Miscellaneous Settings

The various settings here define whether or not you wish to receive reminders when you have emails in the quarantine along with other various settings that change the look of the control panel.

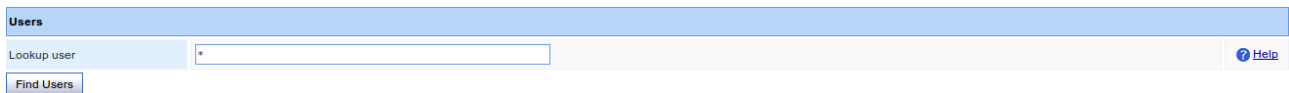
Admin

People who have been given administrative rights to a domain will see an extra menu option to deal with adding new users and configuring default and domain wide settings.

Users

Lookup User

With the lookup user field you can search for and log in as other users of the system.



Users

Lookup user

[Help](#)

Clicking Find Users will take you to a page showing a summary of the cache contents for all emails that have been set up as well as a catch all for all the emails that haven't.

2 Users Found [Help](#)

Username	Non-Spam	Spam	Virus	Banned	Header
@vorari.net	73	23	0	0	0
ryan@vorari.net	0	1	0	0	0

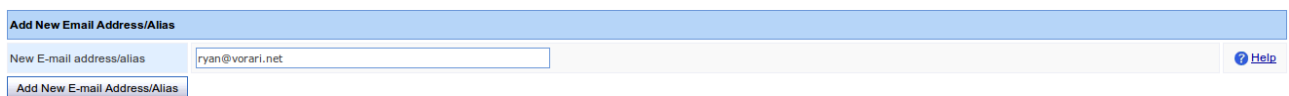
Clicking on a link on the left hand side will log you in as that user and all the cache contents you can see are now for that user. You can tell you're logged in as another user as at the bottom of the Menu bar the user name will change to say:

Username:
Administrator: scott@vorari.net (as
ryan@vorari.net)

The menu bar down the left hand side is now relative to that user, all the settings and the cache contents shown are now for the user you're logged in as, to log back into your own account, either click on Admin in the menu bar down the left hand side, or log out and log back in.

The user @domain.tld is a catch all, any emails received for the domain that there is no user set up for will be added to the cache of this user.

Add New Email Address/Alias



Add New Email Address/Alias

New E-mail address/alias

[Help](#)

To add a new user for the domain you use this field, doing so will allow you to control the settings for that email address separate to the default settings for the domain. When adding a new user they will be sent an email with their login name and password.

Link E-mail Address/Alias

Link E-mail Address/Alias	
E-mail address/alias:	<input type="text" value="ryan@vorari.net"/> <input type="text" value="scott@vorari.net"/>
User account:	<input type="text" value="ryan@vorari.net"/> <input type="text" value="scott@vorari.net"/>
Link E-mail Address/Alias	
Help	

If a user has multiple email addresses then you can link the addresses to their accounts for them, this way they only require one login to the control panel instead of one login per email address. *The same warning applies here in that once you assign an address to a user account, that change can't be undone without removing and re-adding the email address.*

Delete E-mail Address/Alias and Delete Users

The last two parts to the user admin section are where you can delete and add users and email addresses, to do so select the addresses or users you want to delete and click the corresponding button.

Delete E-mail Address/Alias	
E-mail address/alias:	<input type="text" value="ryan@vorari.net"/>
Delete E-mail Address/Alias	
Help	

Delete Users	
User account:	<input type="text" value="ryan@vorari.net"/>
Delete Users	
Help	

Domains

Under the domains admin section you can find a list of all the domains the user you're logged in as has administrative control over. To edit the settings click the Edit Settings button. See the Filter Settings section for more details.

Filter Settings

This is where you configure how sensitive to unsolicited email the filter is. Individual user settings take precedence over domain wide settings, this way if you have specific users or email addresses you wish to have unique filtering options set for you can, otherwise the domain settings get used.

Each filter option has three actions that can be taken when a rule is triggered:

Labelled

When selected, this option tells the email filter to let the email through but to label it as spam by altering the subject of the email and adding *****SPAM***** to it.

Quarantined

When selected, this option tells the email filter to hold the email in quarantine, preventing it from being forwarded on to the recipient. When the user logs into the control panel they will be able to see a list of emails considered to be spam and will be able to release them if they were marked falsely.

Discarded

When selected, this option tells the email filter to discard the email, it's advised rather than outright discard emails it'd would be better to quarantine them, you have the option of deleting them from the cache contents.

Virus Scanning

Filter Settings		Help
Virus Scanning	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Detected viruses should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded	

To enable or disable virus scanning select the relevant radio button, then choose how you want to handle emails that have been detected to contain viruses.

Spam Filtering

The way the spam filter works is every email gets scanned and gets checked for common patterns used by spam senders, including checks for spoofed headers, DNS problems and against lists of known spam senders amongst other checks. Each of these checks has a score associated with it.

For example, emails that have references to an anxiety control drugs are given a score of 1.5.

The scores are tallied up and and if it reaches a score higher than the one specified below, it will perform the action you've asked it to. Generally a score of around 4 or 5 should be about right to avoid most false positives and catch the majority of spam.

Spam Filtering	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Detected spam should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded
Add a prefix to the subjects of spam?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Add X-Spam: Headers when Score is >=	<input type="text" value="1,000"/>
Consider mail 'Spam' when Score is >=	<input type="text" value="5,000"/>
Quarantine Spam when Score is >=	<input type="text" value="5,000"/>

X-Spam headers are headers that are added to the email, most email clients recognise these headers and can be configured to deal with emails appropriately.

For labelling emails with ****SPAM****, select Labeled and change the "Consider mail 'Spam' when Score is >=" to the level you're looking for.

To Quarantine emails select Quarantined and set both the "Consider mail 'Spam' when Score is >=" and the "Quarantine Spam when Score is >=" to the level you're looking for.

The higher the number the more lenient the spam filter a score of around 4 or 5 is a good starting level. You can get an idea of what scores emails are getting and the reason for those scores when looking in the content cache. See the section of this guide labelled Content Cache for more details.

Attachment Type Filtering

Attachment Type Filtering	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Mail with dangerous attachments should be...	<input checked="" type="radio"/> Labeled <input type="radio"/> Quarantined <input type="radio"/> Discarded

If this is enabled emails will be filtered if they contain any of the banned attachment types. Appendix A provides you with the list of attachments types that are filtered.

Bad Header Filtering

Bad Header Filtering	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Mail with bad headers should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded

If enabled any emails containing bad headers will be filtered appropriately.

Domain Specific Filters

Non-spam item caching

Should non-spam items be cached?	<input checked="" type="radio"/> Yes <input type="radio"/> No
----------------------------------	---

When enabled emails that aren't deemed as being spam will be saved to the content cache, this can be useful as it will allow you to train the spam filter.

SMTP IPs

Primary SMTP IP	<input type="text" value="89.16.185.71"/>
Secondary SMTP IP	<input type="text" value="89.16.185.71"/>

Enter the IP addresses of your SMTP server here, this will tell Mailguard where to send the emails once they've passed through it's filtering systems. If you don't have a backup mail server, just enter your primary twice.

Add Administrator

Here is where you can additional Administrators to the domain, adding a user to the Administrator list gives them the same access to the Admin section in the menu.

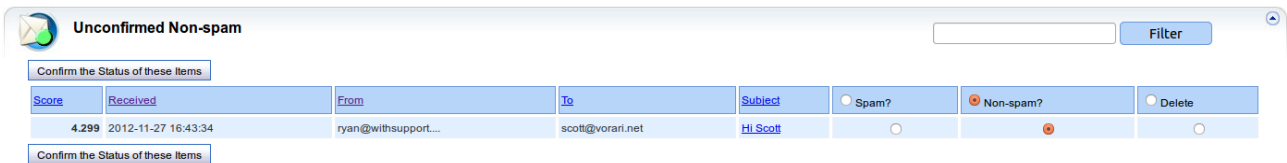
Cache Contents

Mailguard has five separate caches for emails it filters.

- Non-spam Cache
- Spam Cache
- Virus Cache
- Banned File Cache
- Banned Header Cache

Each one is a temporary store for emails that come in, non-spam emails which are delivered straight to the recipient are cached for 5 days, all quarantined emails are kept for 30.

When viewing one of the contents caches you'll be presented with a screen such as this:



This is where you decide what to do with the emails in the cache, you will see a list of all the emails Mailguard has and on the right hand side you can select whether or not the email was spam or not, or to just delete it from the cache.

If you find you're getting emails come through that are spam but aren't being recognised as such you can help train the spam filter by marking them as such here. Doing so gradually trains the Bayesian probability engine of the spam filter to recognise spam emails. Confirming emails as not being spam also does the same. Deleting mail just removes the email and doesn't train the filter one way or another.

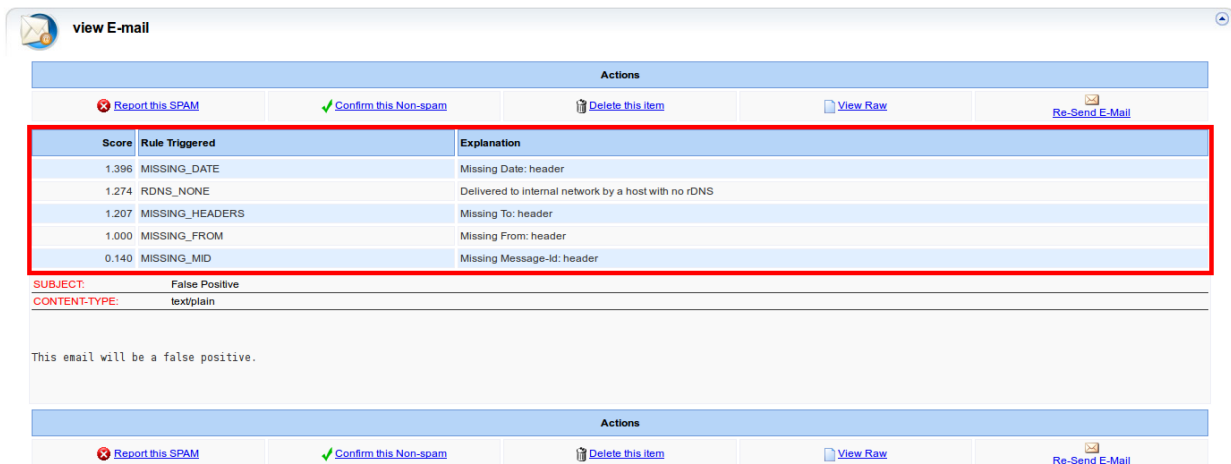
On the far left of the list you can see the score each of the emails received by the Mailguard filter, using these values will help you decide on a suitable level of protection for your filtering settings.

If you click on the email subject you are able to view the email, at the top of this page you can see a list of all the rules that were hit and the scores they have associated with them, this will help you understand why an email is being marked as spam.

You can narrow down the list of emails shown by using the filter text box in the top right.

Email View

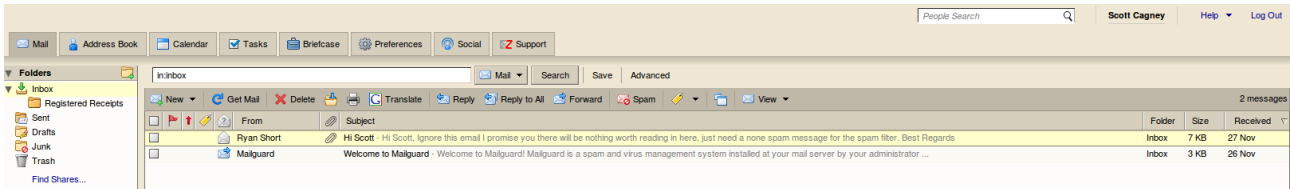
Clicking on the subject title of an email will allow you to view the email in the browser, at the top of the email is a list of rules triggered by this email and the scores associated with those rules, you can see these shown in the red box in the picture below.



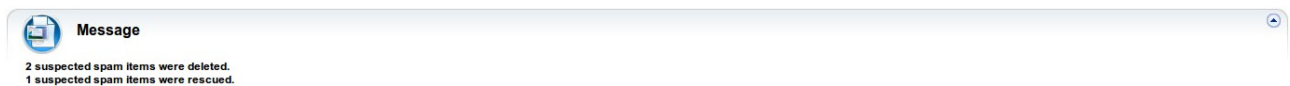
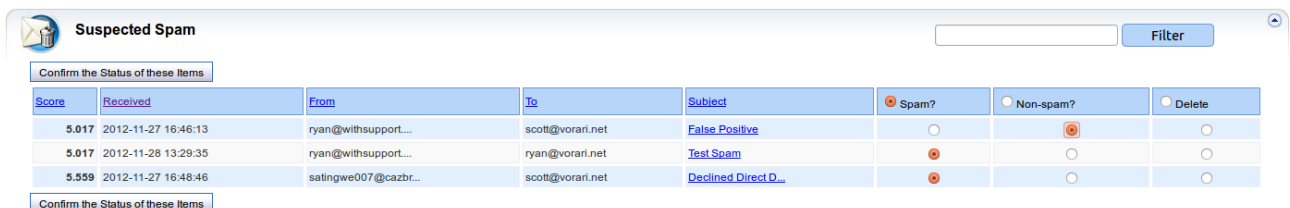
Releasing Quarantined Email

In the example below one of the emails is a false positive that has been quarantined, to release the email simply need to mark it as non-spam and confirm the status of the items. Mailguard will then send out the non-spam emails selected and delete all the spam ones selected, first passing them to its learning algorithms.

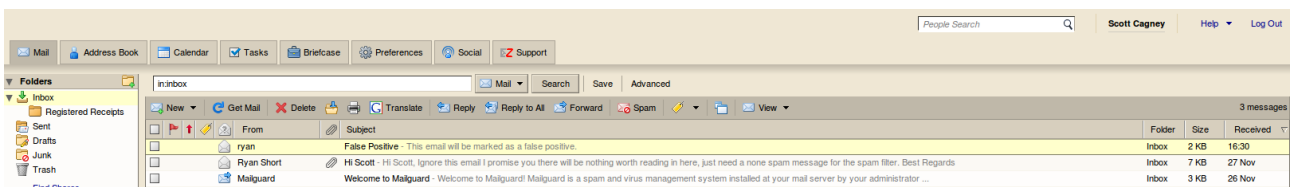
Here's the Inbox before releasing the email.



Then the email is released.



Here's the email received.



Using the Service – MX Records

To actually have your email be filtered by the Mailguard service, once you have everything set up the way you want it, and most importantly the SMTP settings on the domain page correct, you need to point your MX records to "mailguard.vorari.net.". You can do this by logging into your DNS providers control panel and following their instructions on how to add/edit MX records.

Appendix A – List of filtered attachments

ade
adp
app
bas
bat
chm
cmd
com
cpl
crt
exe
fxp
hlp
hta
inf
ins
isp
js
jse
lnk
mda
mdb
mde
mdw
mdt
mdz
msc
msi
msp
mst
ops
pcd
pif
prg
reg
scr
sct
shb
shs
vb
vbe
vbs
wsc
wsf
wsh
mim
b64
bhx
hqx
xxe
uu
uue
exe-ms
lha
cab
dll