Adam Internet Pty Ltd (ABN. 22 055 495 853)
Street Address: Level 7, 117 King William Street, Adelaide 5000
Postal Address: GPO Box 121, Adelaide 5001
Business Solutions (08) 8423 4020 Fax (08) 8231 0223
Email: business@adam.com.au

USAGE GUIDE

ADAM INTERNET SPAM FILTER MANAGER

Adam Internet Pty Ltd (ABN. 22 055 495 853)
Street Address: Level 7, 117 King William Street, Adelaide 5000
Postal Address: GPO Box 121, Adelaide 5001
Business Solutions (08) 8423 4020 Fax (08) 8231 0223
Email: business@adam.com.au

Introduction

For all Business Domain hosting services, Adam Internet provides the ability to add SPAM and VIRUS filtering. This service reduces the amount of "garbage" mail that seems to be so common these days.

This guide aims to introduce you to our Spam Filter Manager, which is the online tool you can use to manage and maintain your Spam Filter settings.

While the system is quite easy to use and has comprehensive help available while you're using it, we have created this setup guide so you can print it and keep it handy for your reference.

How the Spam Filter works

The Adam Internet SPAM Filter works in two ways to catch junk mail.

- The first series of steps is related to security of the sending server. Every host on the Internet has a "rule book" known as the RFCs, to which they are supposed to (but not obliged to!) abide. If you have Spam Filtering enabled, we make sure they abide by the rules. This helps to weed our servers that are insecure, or are forging their identity (for example, pretending to be the Hotmail server).

- The second step is to do with email content – profanity, pornography, words such as "viagra" or "cheap meds" etc. An email message scores points on a 1 to 10 scale, and currently if it scores more than 6 it's filtered. If it scores less than 6 we will let it pass through the filter – this explains why some junk will still get through, and also explains why sometimes a legitimate message may be filtered.

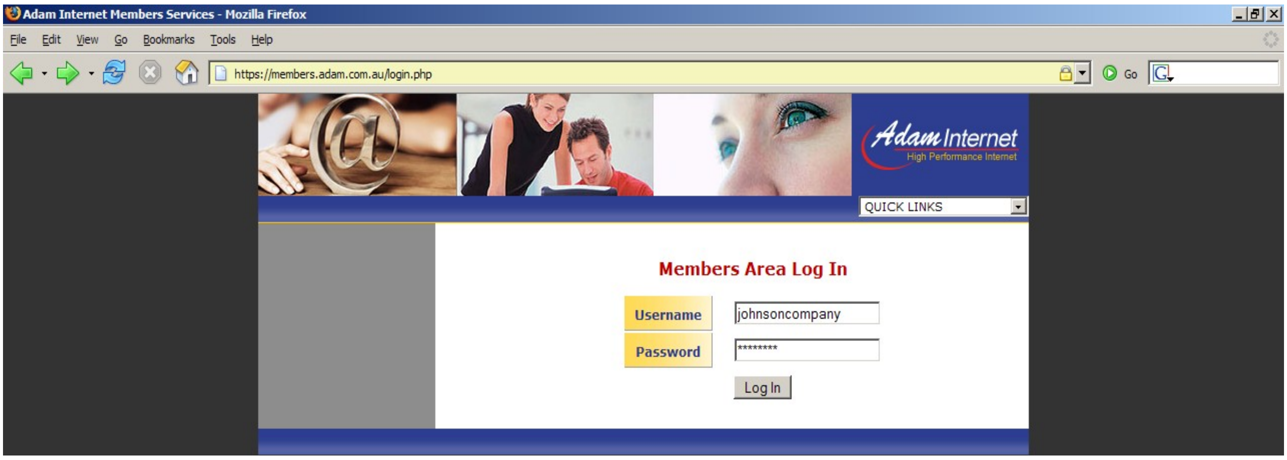
Using the Spam Filter Manager

The Spam Filter Manager is our online tool you can use to view a list of any mail that has been caught as junk. This will show you how effective the filter is, and also provide a means to ensure we're not incorrectly catching any legitimate mail.

Note if some legitimate mail is filtered, it's simply because it broke one of the rules detailed in this guide. If you can't get the sender to fix the rule-breaking problem at their end, you can "whitelist" that sender which will prevent them from being filtered again for up to one year.

The Spam Filter Manager is accessed via our member services area – http://members.adam.com.au

Simply log into this site with the primary username of your business account. If you don't know the primary username, please call or email so we can advise you.



Adam Internet Members Services - Mozilla Firefox

https://members.adam.com.au/login.php

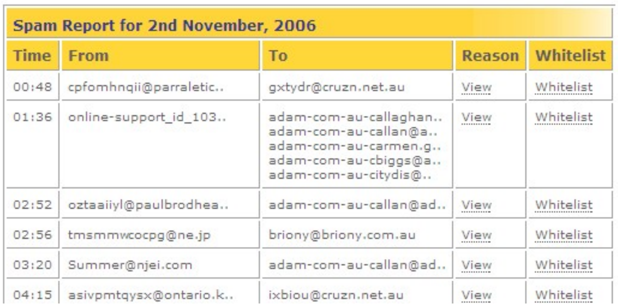
Members Area Log In

Username: johnsoncompany

Password: ********

Log In

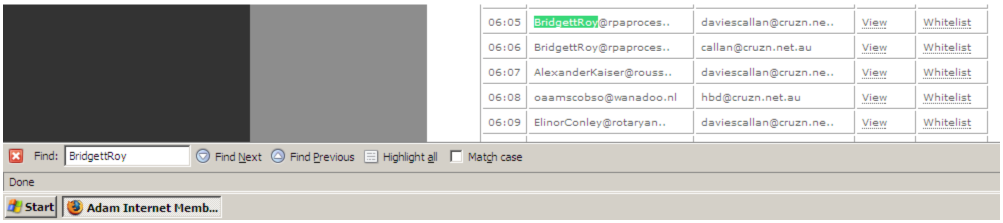
Once you're logged into Member Services, click SPAM FILTER MANAGER on the left. Please note this page may take some time to load, especially if we've caught a lot of Spam for you. Once the page has loaded you'll see a list of all today's mail that has been filtered as Spam. If you want to see yesterday's list, there's a link right at the bottom of the page. The list looks something like this :



Spam Report for 2nd November, 2006

Time	From	To	Reason	Whitelist
00:48	cpfomhnqii@parraletic..	gxtydr@cruzn.net.au	View	Whitelist
01:36	online-support_id_103..	adam-com-au-callaghan.. adam-com-au-callan@a.. adam-com-au-carmen.g.. adam-com-au-cbiggs@a.. adam-com-au-citydis@..	View	Whitelist
02:52	oztaaiiyl@paulbrodhea..	adam-com-au-callan@ad..	View	Whitelist
02:56	tmsmmwcocpg@ne.jp	briony@briony.com.au	View	Whitelist
03:20	Summer@njei.com	adam-com-au-callan@ad..	View	Whitelist
04:15	asivpmtqysx@ontario.k..	ixbiou@cruzn.net.au	View	Whitelist

If your list is really huge, it might be difficult to find a particular sender's address in there. You can use the FIND function on your Web Browser's EDIT menu to search for someone's email address. If you're using Firefox (the most secure Web Browser), your FIND TEXT option will look something like this :



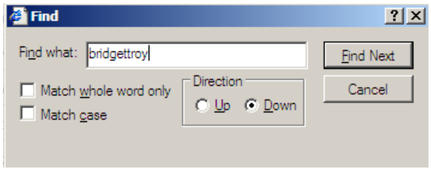
06:05	BridgettRoy@rpaproces..	daviescallan@cruzn.ne..	View	Whitelist
06:06	BridgettRoy@rpaproces..	callan@cruzn.net.au	View	Whitelist
06:07	AlexanderKaiser@rouss..	daviescallan@cruzn.ne..	View	Whitelist
06:08	oaamscobso@wanadoo.nl	hbd@cruzn.net.au	View	Whitelist
06:09	ElinorConley@rotaryan..	daviescallan@cruzn.ne..	View	Whitelist

Find: BridgettRoy

☐ Match case

Done

If you're using Internet Explorer, your FIND TEXT option will look something like this :



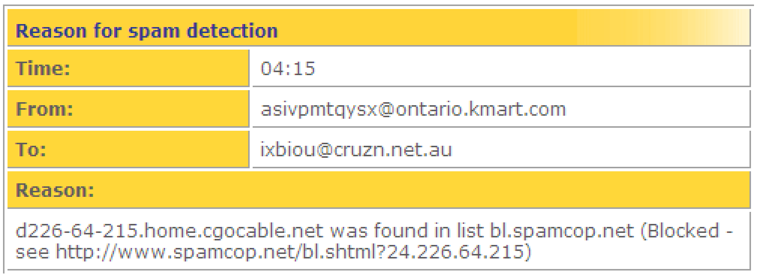
Find

Find what: bridgettroy

☐ Match whole word only
☐ Match case

Direction
○ Up ● Down

Next to each entry, you'll see two options – VIEW and WHITELIST. If you click VIEW, the area at the top of the screen will update to show you more details, including the reason that the message was filtered :



Reason for spam detection

Time:	04:15
From:	asivpmtqysx@ontario.kmart.com
To:	ixbiou@cruzn.net.au
Reason:	

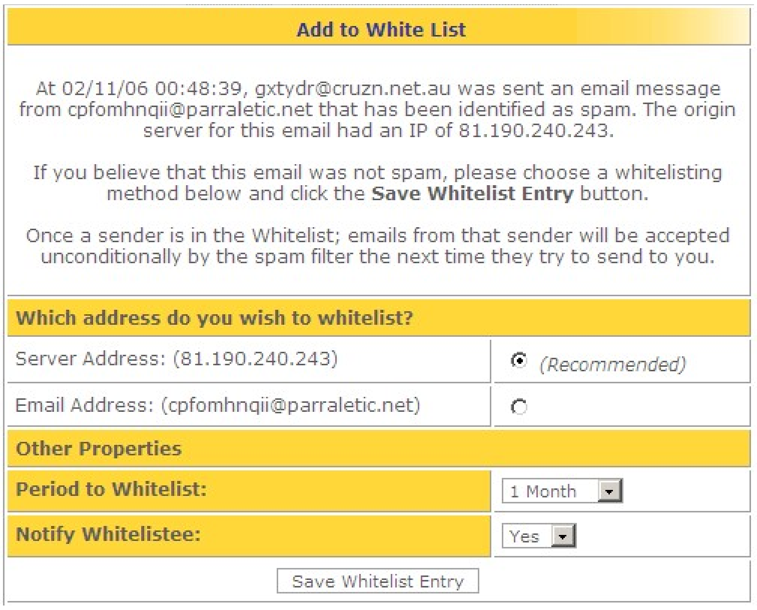
d226-64-215.home.cgocable.net was found in list bl.spamcop.net (Blocked - see http://www.spamcop.net/bl.shtml?24.226.64.215)

It's really important that you take careful note of this error, as you'll probably want to let the sender know about it so they can ask their company or Internet Provider to fix the problem. The error message may also include a website address, as per the above example. If it does, you might want to copy and paste that into your Web Browser, as this will give you some more information about the reason it was blocked.

Later on in this guide, is a list of the possible error messages aswell as explanations so you can understand what causes these and what you can do to fix it.

<u>The Whitelist</u>

If you find that messages from one particular person or company are being filtered, and you don't want them to be, you can use the <u>whitelist</u> function to make sure those messages always get to you. Just click the WHITELIST option next to the particular entry in the list, and you'll see a screen similar to this one :



Add to White List

At 02/11/06 00:48:39, gxtydr@cruzn.net.au was sent an email message from cpfomhnqii@parraletic.net that has been identified as spam. The origin server for this email had an IP of 81.190.240.243.

If you believe that this email was not spam, please choose a whitelisting method below and click the **Save Whitelist Entry** button.

Once a sender is in the Whitelist; emails from that sender will be accepted unconditionally by the spam filter the next time they try to send to you.

Which address do you wish to whitelist?

Server Address: (81.190.240.243)	● *(Recommended)*
Email Address: (cpfomhnqii@parraletic.net)	○

Other Properties

Period to Whitelist:	1 Month
Notify Whitelistee:	Yes

The text at the top tells you some brief details about the message. You'll also get the choice to whitelist either a Server Address, or an Email Address.

- If you choose <u>Server Address</u> then it means that ALL mail from this particular server, regardless of email address, will be whitelisted. Remember that large companies or Internet Providers may run several servers, in which case whitelisting one of them won't whitelist the others – you might find the messages keep getting caught until you've eventually whitelisted all the servers at that location. To give you some idea of network size, Adam Internet has 4 mail servers for outgoing mail and 7 for incoming mail, therefore you can imagine some overseas providers may have upwards of 30 or 40 mail servers!

- If you choose <u>Email Address</u> then it means that all mail from that particular address, regardless of mail server, will be whitelisted. This means that you won't have to whitelist multiple servers, however if another person at that company or Internet Provider tries to email you, the message will be filtered and you'll need to whitelist that email address too.

Generally, it's best to whitelist a SERVER as opposed to an ADDRESS, but the choice is yours.

When you've made your choice above, choose how long to whitelist for, and click the SAVE WHITELIST ENTRY button.

When the time is up for that whitelist, we'll email you and offer to renew the whitelist. Note that we'll email the “contact” address on your account, which is not necessarily yours – it might be someone in your accounts department.

Since you're already in Member Services, you can use the “contact manager” option to check which email address we'll use for notifications, and change it if you need to. If you do change the contact address, remember this is where we send ALL notifications, including invoices etc.

Adam Internet Pty Ltd (ABN. 22 055 495 853)
Street Address: Level 7, 117 King William Street, Adelaide 5000
Postal Address: GPO Box 121, Adelaide 5001
Business Solutions (08) 8423 4020 Fax (08) 8231 0223
Email: business@adam.com.au

Description of Spam Filter error messages

We have prepared a summary of the errors/reasons you may see in the Spam Filter. We have included a plain language explanation as to what these messages really mean, and what you have to do in order to resolve the problem.

Remember, the whitelist is only a “patch” solution, the real problem still needs to be resolved at the sender's end and if nobody notifies the sender that there is a problem, they'll never know to fix it.

The error descriptions below are listed as follows :

Error Type

- example error message 1
- example error message 2

Explanation: a plain English explanation of the error message

Solution: a recommendation as to what you should do in order to get the problem properly resolved

Bad or Forged Server Identification

- dropped due to bad HELO string "203.6.132.79"
- c-24-1-73-244.hsd1.tx.comcast.net dropped due to bad HELO string "localhost"

Explanation: When a mail server wishes to exchange mail with another mail server, they start the conversation with a HELO string, as if to say HELLO, I am the mail server at adam.com.au. If a remote server provides us with incomplete information (for example HELLO, I am the server at no-name) or incorrect (for example pretending to be the Hotmail server), we will reject the mail as SPAM.

Solution: This error should be relayed to the sender of the blocked email, as it's most likely caused by a configuration problem at their Internet Provider or company mail server. This can happen purely by mistake, or can be a deliberate attempt by the sender to conceal their identity (in which case you need to ask why they do not wish to be identified).

Sending Server is in a Black List

- 68-68-251-14.atlsfl.adelphia.net was found in list sbl-xbl.spamhaus.org (http://www.spamhaus.org/query/bl?ip=68.68.251.14)
- dsl-200-95-47-223.prod-infinitum.com.mx was found in list sbl-xbl.spamhaus.org (http://www.spamhaus.org/query/bl?ip=200.95.47.223)
- was found in list relays.ordb.org (This mail was handled by an open relay - please visit)
- was found in list dnsbl.njabl.org (open proxy -- 1109132611)

Explanation: If a mail server is known to have been the source of a lot of SPAM in the past, it may have found its way onto an email blacklist. Many Internet Providers (including Adam Internet) subscribe to these blacklists to obtain a list of likely SPAM sources. If the remote server is on one of these lists, the mail will be dropped as SPAM.

Solution: If the sending server is a source of SPAM, the problem needs to be resolved. Once this has gbeen done, they can apply to the blacklist website in question to have the blocking removed. There will usually be a website address listed on your Spam Filter Manager error message, which you can visit to get more information as to why that server has been blacklisted, and how the blacklist can be removed. You should definitely send this information to the sender of the blocked email so they may get the problem fixed, as there are probably a LOT of places that they cannot send email to!

DNS Mismatch

- (failed to find host name from IP address)
- (72.3.245.46 does not match any IP address for www.magnonsolutions.com)
- Reverse DNS is not set up correctly for this Host

Explanation: Every server on the Internet has an IP Address, a unique numerical identifier such as 203.123.456.789. Each IP Address should have a name attached to it, such as mail.adam.com.au, or www.adam.com.au. If a remote server wishes to send email to our network, we will check that their IP Address matches their name, and then do a reverse check to make sure that the name matches the IP Address. If the two checks don't match up, we will reject the mail as SPAM.

Solution: This error should be relayed to the sender of the blocked email, as it's most likely caused by a configuration problem at their Internet Provider or company mail server. This can happen purely by mistake, or can be a deliberate attempt by the sender to conceal their identity (in which case you need to ask why they do not wish to be identified).

SPF Lookup problems

- wiley-334-3914.roadrunner.nf.net dropped due to bad SPF check (squall.mail.adnap.net.au: domain of excite.com does not designate 205.251.144.189 as permitted sender)

Explanation: This is just like the DNS Lookup problem detailed above, however SPF is a slightly more robust and secure way of validating a server's identity. SPF essentially lists the servers that should be sending mail for that domain – for example mail from @adam.com.au should only originate from the Adam Internet mail server. If it comes from somewhere else, it's probably forged. If the SPF check fails, we will reject the mail as SPAM.

Solution: This error should be relayed to the sender of the blocked email, as it's most likely caused by a configuration problem at their Internet Provider or company mail server, or perhaps the sender with their computer configured incorrectly.

Bad or Missing Recipient Address

- cpe-203-45-63-18.vic.bigpond.net.au had a bad To address ()

Explanation: The BCC option in your email software can be used to send email to many recipients, without those recipients being able to see who else you sent the message to. Some people use the BCC field to send jokes or videos to their friends, and some businesses may use this as a “cheap” way of sending newsletters etc (instead of buying a real mailing list server). If this is done, and the TO field is empty, the email does not abide by the RFC rules which state that an email must have a Recipient, a Sender, a Subject, and the Message itself.

Solution: You should ask the sender to make sure that there is a valid email address in the TO field. The easy way around this is to continue doing the BCC as they always have, however just put their own email address in the TO field. They can still keep everyone else in BCC which keeps all the email addresses private, just having themselves in the TO field prevents the Spam filter from deleting the message.

Banned Attachment(s)

- had a file with extension "exe" attached
- had a file with extension "scr" attached

Explanation: Due to the increasing number of viruses and other nasties on the Internet, our SPAM Filter will block emails that contain Windows Executable attachments (ie. programs). Examples of these are file names that end in .exe, .com, .bat, .pif, .scr, .vbs, plus a few others. As a general rule, 90% of mail that contains files like this, are viruses! Additionally, even if it's not a virus it's still a big risk, as a program can do anything it's written to do - for example it can wipe your whole computer. And once you click it, there's no stopping it. This is why we block these types of files.

Solution: If you wish to receive this type of material via email, you might ask the sender to ZIP it first using the free trial software at www.winzip.com. Or, ask them to make this available for download on their website, even the free web space they get from their ISP!

Thank You!

Thankyou for taking the time to read our guide for Domain Email Manager. If you have any questions or suggestions, please contact us via business@adam.com.au, or telephone (08) 8423 4020.