



Symantec Antivirus and Antispam

Antivirus and Antispam support guide

Version 1.0



Contents

1 Checking Symantec IP's	2
Checking the network address - What's my IP?	2
2 Setting the proxy in your browser to point directly to Symantec	2
3 Testing the Antivirus and Antispyware services	2
4 Configuring Antivirus alert notifications	3
5 Releasing Mail from Anti-Virus	3
6 Spam Detection Settings	5
Detection Settings	5
7 Spam Manager Email Aliases	6
Managing aliases.....	6
8 Managing your approved and blocked senders lists Depending on your organisation's Email Services configuration, you may not be able to manage your own approved and blocked senders lists. In this case, you will not see the Approved Senders and Blocked Senders tabs in Spam Manager.	7
Viewing your approved and blocked senders	8
Adding an approved or blocked sender	9
To add an approved or blocked sender:	9
To add an approved sender when you release a message from Spam Manager	9
Editing an approved or blocked sender	10
To delete selected approved or blocked senders:	10
To delete all approved or blocked senders:	11
9 I have released a message but not received it in my inbox	11
10 I have not received an email asking me to register and log in	11
11 Setting Spam Manager notification options If the notification facility has been enabled by your organisation, you will receive periodic email notification of any spam held by Spam Manager. Each notification email lists only those messages received by Spam Manager since the previous notification.	11
To change the frequency of notifications:	12
12 Spam Manager account groups	12
13 Managing your messages	12
Viewing messages in Spam Manager	12
Searching for a message.....	13
Selecting messages	14
Releasing messages	15
To release a message from Spam Manager	15
Deleting messages	17

Setup

1 Checking Symantec IP's

Set the firewall rules using the IP's given by Symantec. Next, test the firewall rules using Pings and a Telnet Session.

Please note, if you are unable to bring up a command window and perform a ping or Telnet session, visit Microsoft to search for instructions on how to fix this.

[Click here to view the tutorial](#)

Checking the network address - What's my IP?

If the external IP of your network is not registered with the service, the service will reject any traffic from that IP source. We can show you how to check your external IP by using www.whatismyip.com if necessary.

[Click here to view the tutorial](#)

2 Setting the proxy in your browser to point directly to Symantec

The proxy settings of a test machine will be configured so that the web traffic from the machine is forwarded to the Symantec Infrastructure to be processed. The reason for performing the implementation on a test machine is to ensure that the rest of the machines on the network will not be affected.

[Click here to view the tutorial](#)

3 Testing the Antivirus and Antispyware services

This test is to check the AntiVirus and Anti-Spyware services you have bought which is part of the URL filtering. This will involve downloading a HTTP Anti-Malware test file. It is specifically for testing purposes. However, if for some reason the services fail to pick up the virus, then the file can be easily removed using standard network Anti-Virus software.

You do not have to perform this test if you do not wish to, Claranet SOHO is not responsible for any situation that might occur if you are unable to remove this file.

[Click here to view the tutorial](#)

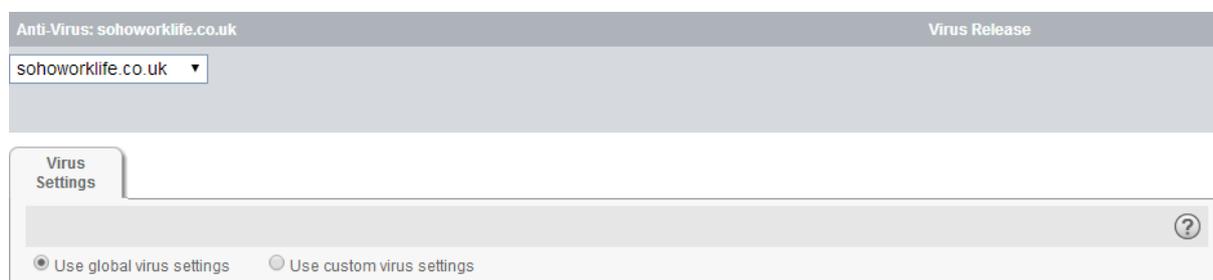
Troubleshooting

4 Configuring Antivirus alert notifications

When mail is detected by the antivirus system, an alert mail can be sent to both the recipient and the administrator of the domain.

By default, all admin addresses will be configured to be the same as the main portal administrators email address. However, there may be a need for specific users of each domain to be notified if mail release is required.

To change the administrator address for antivirus detection, navigate to the **Antivirus** section of the [portal](#), select the domain which requires modification from the drop down list, or if this is for all domains select the global option and confirm that the domain is set to use custom virus settings (if this domain requires an alternate admin email address from the global settings).



Anti-Virus: sohoworklife.co.uk Virus Release

sohoworklife.co.uk

Virus Settings

Use global virus settings Use custom virus settings

Enter the new administrator email address into the provided field.

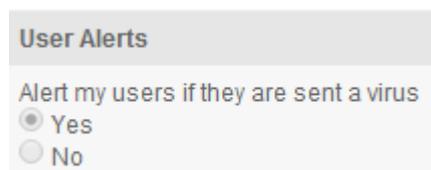


Administrator Alerts

Enter an administrator's email address for virus alerts

Maximum length 255 characters.

If you wish for the intended recipient of the email to be notified when a virus is detected then select **yes** under **User Alerts**.



User Alerts

Alert my users if they are sent a virus

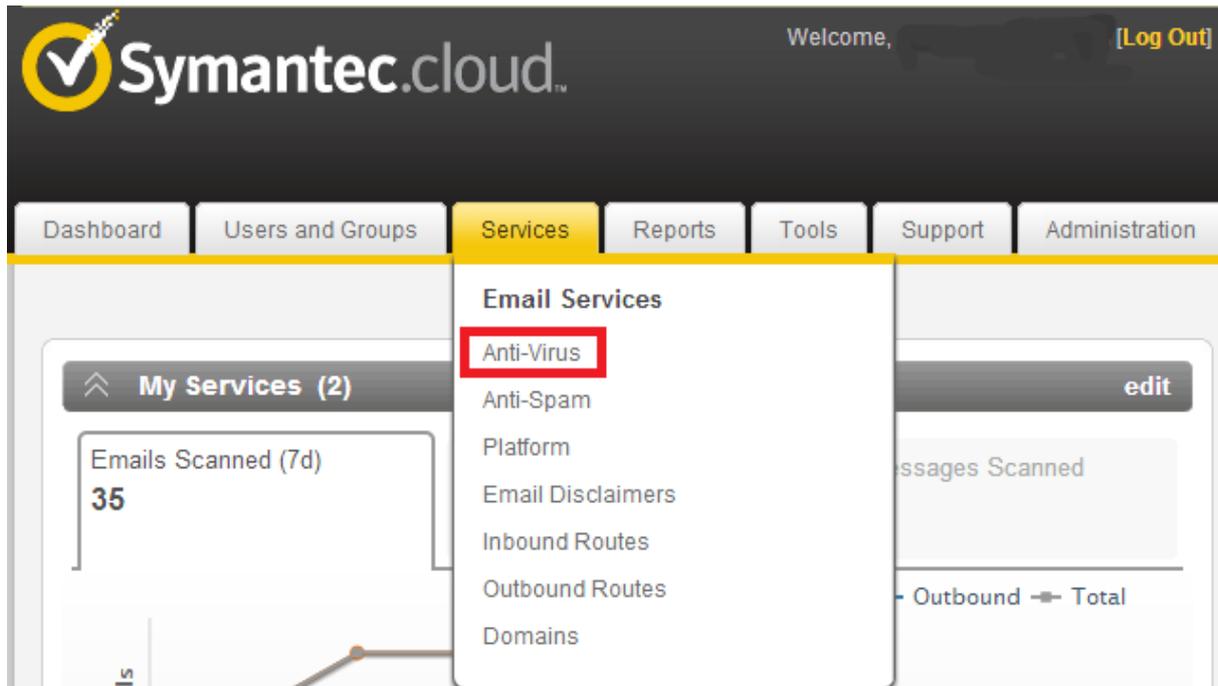
Yes No

Check that the mail limits are configured as required for this domain and then select **save and exit**.

5 Releasing Mail from Anti-Virus

Once logged into Symantec.cloud, you will need to navigate to the **Services** tab.

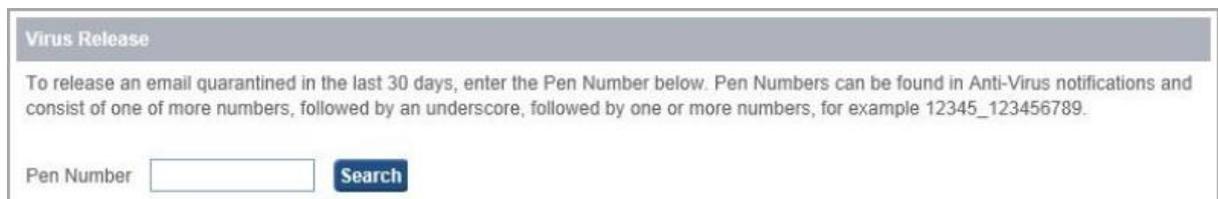
Hovering over the tab will provide a list of options. In this instance we are looking for the **Anti-Virus** page.



To release emails that have been classified as a virus, click **virus release** in the top right corner of the dashboard.



When selected, a new window will open which allows for a **PEN ID** to be entered. This is the unique ID for the mail in question and can be found on either the administrator notification, the recipient notification or can be provided by our support team following a trace of the email in question (sender, recipient, date/time and subject will need to be provided in order for the support team to track the mail and retrieve the PEN ID).



Once the PEN ID has been entered, the mail will then be released to the original intended recipient.

Mails are released at the users own risk. If you believe mails are being detected incorrectly, it is possible to submit them to Claranet SOHO for re-assessment by Symantec. The more signatures that are correctly identified the better Symantec's scanners become.

6 Spam Detection Settings

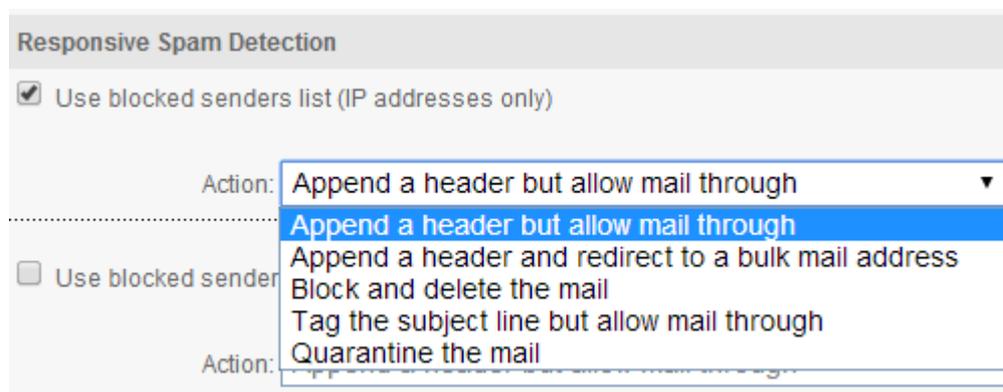
Detection Settings

When you have navigated to the anti-spam homepage (Services > Anti-Spam), click on the **Detection Settings** tab.



The first option you can choose is if you wish to use the approved senders list which you would have set up. This can be either the IP or Domains and e-mail address only or use both of them. You can assign to use the SPF function which explains what it does next to the ticket box.

The following option allows you to choose how Symantec will deal with the spam mail; this can be by the option in the drop down box.



You have the option of using the Skeptic Heuristics which is part of Symantec that checks everything in the mail header to make sure the mail has come from the right location. You can also choose how Symantec deals with this mail.

Bulk Mail Address

Please specify the address that mail identified as spam will be forwarded to if the **Append a header and redirect to a bulk mail address** action is selected.

Enter an email address:
Maximum length 255 characters

Subject Line Text

Enter the text that will appear on the subject line of emails tagged as spam

Enter text:

Put this text in front of the subject line
 Put this text at the end of the subject line

In the **Subject Line Text** section, you can customise how the subject line will appear for emails tagged as spam.

If you change your settings to quarantine spam emails, the intended recipient will be sent an email, informing them that an email is in quarantine along with a link to view the email.

7 Spam Manager Email Aliases

Managing aliases

If you have several email addresses within your organisation (for example, john.smith@example.com and jsmith@example.com), you can combine these as aliases under a single Spam Manager account.

You will only need one set of login details (email address and password) for Spam Manager and all your spam will be displayed together.

Please note, you can only use email addresses that have been registered by your organisation as aliases.

If you have set up aliases for your account, the **Summary page** in Spam Manager displays both the sender and the recipient of your spam messages.

To add an alias:

- Login to the Spam Manager account to which you would like to add an alias.
- Click the **Options** tab.
- Click the **Manage Aliases** link.
- In the Add an alias box, enter the additional email address to be managed by this account.

Spam Manager Symantec.cloud

Summary Approved Senders Blocked Senders Options

You can search for an email by *Sender* or *Subject*. Please enter your search text below.

Sender	Subject	Date Received	Size
<input type="checkbox"/> mailer@	Bring this camera on your next vacation	6/9/16 10:18 AM	22941
<input type="checkbox"/> mailer@	Viarexin	6/9/16 10:17 AM	3887
<input type="checkbox"/> mailer@	Unbelievable camera takes pictures that are 20 ...	6/9/16 10:17 AM	25554
<input type="checkbox"/> mailer@	Viarexin -	6/9/16 10:14 AM	3883

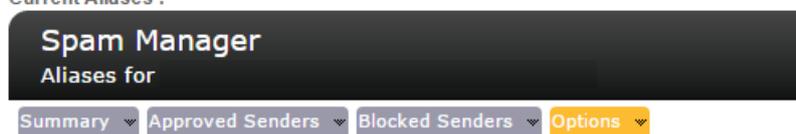
All times are displayed in UTC

- Click the **Add** button, then a confirmation message is displayed. A message is also sent to your other email address, requesting confirmation that this email address should become an alias.
- Click the URL in the message to confirm the creation of the alias. Until you have done this, the alias is shown as 'pending' in Spam Manager.

To delete an alias:

- Login to the Spam Manager account to which you would like to delete an alias.
- Click the **Options** tab.
- Click the **Manage Aliases** link.
- Select the checkbox to the left of the alias to delete.

Current Aliases :

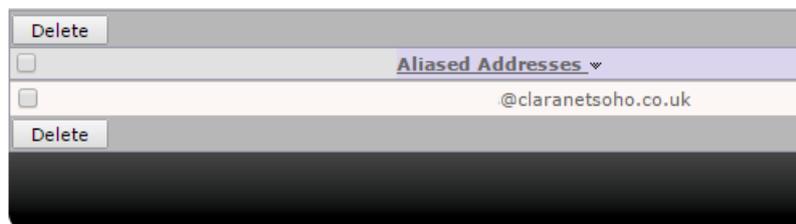


Manage Aliases

If you have several email addresses within your organization (for example john.smith@claranetsoho.co.uk) Before an email address can be added to this account as an alias it must be validated.

Add an Alias :

Enter an email address



- Click the **Delete** button. After an alias has been deleted, any spam received for that email address will no longer be directed to the alias' owner, but will instead be directed to a new Spam Manager account for that email address.

If Spam Manager has been configured to send welcome messages, when spam is received, a message inviting the user to register with Spam Manager is sent to the previously aliased email address. The user will then be able to request a password and manage their own Spam Manager account.

8 Managing your approved and blocked senders lists

Depending on your organisation's Email Services configuration, you may not be able to manage your own approved and blocked senders lists. In this case, you will not see the Approved Senders and Blocked Senders tabs in Spam Manager.

An approved senders list is a list of domain names or email addresses that you want to receive email from, even though these senders may otherwise be blocked by public or company block lists or other spam detection methods.

A blocked senders list is a list of domain names or email addresses that you want to block emails from, if such mail does not typically get intercepted as spam by the Anti-Spam service scanners.

Your organisation may have company approved and blocked senders lists set up. If you are able to manage your own lists, the Email Services Administrator will have specified whether the company lists override your personal lists or vice versa.

If you have any concerns about unwanted email getting through to you or wanted email not getting through to you, contact your Email Services Administrator.

Entries on the approved and blocked senders' lists can be either full email addresses or domains, for example, jsmith@domain.com or domain.com.

The maximum number of entries in your personal approved and blocked senders' lists is 150 in each.

Please note, you should not put your domain name in your own approved senders list—this could cause problems with spam from spoofed email addresses not being quarantined as expected.

Viewing your approved and blocked senders

Click the **Approved Senders** or **Blocked Senders** tab, as required.

The existing entries on your list are displayed, including the sender or domain name, whether the entry is a full email address or a domain, the entry description and the date the entry was added.

The screenshot shows the Symantec Antispam interface. At the top, there are four tabs: 'Detection Settings', 'Quarantine Settings', 'Approved Senders', and 'Blocked Senders'. The 'Approved Senders' tab is selected. Below the tabs, there is a section titled 'Global Approved Senders' with a help icon. A note states: 'This list applies at global level. Emails from senders on this list will be delivered to the intended recipient, unless settings at a group or user level dictate otherwise.' Below this, there is a search field labeled 'Domain/Email/IP' with a 'Search' button. There are also buttons for 'Add entry', 'Delete', 'Upload', and 'Download'. To the right, there is a dropdown menu for 'Entries per page' set to 20. Below the search and buttons, it says 'Showing 1 - 20 of 101.' and navigation links: '<< First | < Previous | Next > | Last >>'. A table is displayed with the following columns: 'Domain | Email | IP', 'Type', 'Description', 'Date Amended', and 'Edit'. The table contains one entry: ':com' (Type: Domain, Date Amended: 27 Apr 2005 7:54 PM, Edit link).

You can sort the list by clicking on the column heading and change the number of items displayed on a single page by using the Entries per page drop-down list and you can locate an entry by searching for a specific sender.

*Please note: You can use partial matching—you do not have to enter the complete email address or domain. You cannot use wildcards in this search field. Entering a * will only find emails that contain the * symbol itself in the sender field.*

Search for senders added to the approved or blocked senders list between two dates and scroll through the pages on the list. To view all entries again after a search click the **Clear Search** button.

Adding an approved or blocked sender

Entries on your personal approved and blocked senders lists can be added in a number of ways:

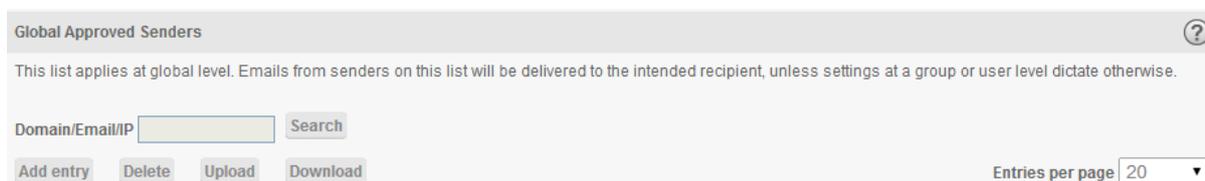
You can add entries to your approved and blocked senders' lists manually in the **Approved Senders** and **Blocked Senders** tabs.

When you release a spam message to your inbox, you can approve the sender of the spam message at that time. You can also approve the sender's domain, so that any emails sent from the domain will bypass the Anti-Spam service.

Your Spam Manager Quarantine Administrator can add, edit, and delete entries on your behalf.

To add an approved or blocked sender:

- Click the **Approved Senders** or **Blocked Senders** tab, as required.
- Click the **Add Entry** button and the Add Sender page will be displayed.



- Enter the email address or domain name of the sender to add to the list. An email address must be the full address with a valid domain name, such as **broberts@shopping.com**. Partial email addresses, such as broberts@shopping, are not valid.

A domain name can be a full name, such as example.com, or a top-level domain, such as .com or .uk. Subdomains, such as name.domain.com, are also valid. Partial domains without the top-level domain, for example, messagelabs or webcam, are not valid. The * wildcard is also not valid within a domain name.

- Enter a description for the entry (this is mandatory).
- Click **Save** and the new entry will be displayed in the list.

To add an approved sender when you release a message from Spam Manager

When you receive a message identified as spam from a sender that you wish to add to your personal approved senders list, select the message, and click the **Release** button.

In the Message released confirmation, click the **Approve sender** or **Approve domain** button, as required.

Spam Manager
Message Released for

Summary | Approved Senders | Blocked Senders | Options

Message released

The message from sender mailer@

Further messages from this sender might still be detected as spam. If you wish to receive messages from this sender in future, please click Approve Sender below.

Note that if your organization has an email security policy in place, it may override your local approved and blocked senders lists. If you release an email and do not

Approve sender | Approve domain | Continue

Copyright © 2014 Symantec Corporation. All rights reserved.

The Add Entry page is displayed with the Sender box already filled in. Enter a description for the entry (mandatory). Click **Save** and the new entry will be displayed in the list.

Editing an approved or blocked sender

To edit an approved or blocked sender:

- Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
- Locate the entry of interest and click on **edit** at the far right of the row.

<input type="checkbox"/>	Domain Email IP	Type	Description	Date Amended	
<input type="checkbox"/>	com	Domain		27 Apr 2005 7:54 PM	Edit

- Edit the email address or domain name, if required. An email address must be the full address with a valid domain name, such as broberts@shopping.com. Partial email addresses, such as broberts@shopping, are not valid. A domain name can be a full name, such as example.com, or a top-level domain, such as .com or .uk. Subdomains, such as name.domain.com, are also valid. Partial domains without the top-level domain, for example, messagelabs or webcam, are not valid. The * wildcard is also not valid within a domain name.
- Edit the description for the entry (this is mandatory).
- Click **Save**. Deleting approved or blocked senders

You are not asked to confirm deletion when deleting entries from the approved and blocked senders' lists.

To delete selected approved or blocked senders:

- Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
- Locate the entries of interest and select the checkboxes to the left of the entries.
- Click the **Delete** button.

To delete all approved or blocked senders:

- Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
- Select the checkbox in the heading of the left column. All entries are selected.
- Click the **Delete** button.

9 I have released a message but not received it in my inbox

The time it takes for a message to reach your inbox depends on a variety of factors that are independent of the Symantec.cloud Anti-Spam service, such as Internet delays.

Please wait for two hours and then release the message again. If it still does not reach your inbox, contact your Quarantine Administrator.

10 I have not received an email asking me to register and log in

If you have not yet received any registration or login details, there are two likely reasons:

You have not received any spam or instead of creating an individual Spam Manager account for you, your Quarantine Administrator has decided to manage your spam in a different way.

However, if you would like to check whether an account has been created for you:

- Go to the login page.
- Click the **Forgot your Password**.
- Enter your email address.
- Click **Password Reset**.

If you receive the error message 'Invalid email address', you do not have a Spam Manager account. If you think you should have a Spam Manager account, contact your Quarantine Administrator.

Or if you receive a password message, click on the link and enter the new password. If no spam has been redirected to Spam Manager, the message 'You currently have no spam in the quarantine system' is displayed.

11 Setting Spam Manager notification options

If the notification facility has been enabled by your organisation, you will receive periodic email notification of any spam held by Spam Manager. Each notification email lists only those messages received by Spam Manager since the previous notification.

The notification email will be in the language that either has been configured by your IT administrator or that you last selected in Spam Manager.

Depending on how Spam Manager has been set up by your Quarantine Administrator, you may be able to change the frequency with which you receive notifications.

If the **Notifications** link is shown on the **Options** page, you can change the frequency of these messages.

Please note, to trigger the sending of notifications, you may need to register and request a password.

To change the frequency of notifications:

- Click the **Options** tab.
- Click the **Notifications** link.
- Ensure that the Send notifications of newly received spam messages checkbox is selected.
- Select a frequency for notifications to be sent from the **Send notifications when?** drop-down list.
- Click the **Save** button.

12 Spam Manager account groups

Your Spam Manager Quarantine Administrator can assign spam for individual Spam Manager accounts to be sent to the owner of an 'account group'. An account group enables spam for several email addresses to be viewable through one Spam Manager account. The settings for the individual accounts still apply to those individuals' email and the users in the group can still view and manage their spam themselves.

If you have been set up as an owner of an account group, you may receive a notification email advising you of this and requesting your confirmation. The users of the individual email addresses in an account group can still manage their own spam and account settings.

If your spam is managed by someone else as part of an account group, you may receive a notification email advising you of this and requesting your confirmation. You can still view and access your own Spam Manager account and manage your spam and account settings yourself.

13 Managing your messages

Viewing messages in Spam Manager

Once you have logged into Spam Manager, any spam email which you have is listed. Details of the sender and date are shown for each message. Depending on your organisation's security policy, the subject of the message may also be shown.

If your Spam Manager account contains spam from more than one email address; that is, if you have set up an alias, the address to which each message was sent is shown in a Recipient column.

To sort the list:

- Click the **Summary** tab.
- Click the heading of the column to sort by.
- An arrow is displayed in the column heading to indicate the direction of the sort.
- To define the number of entries displayed on a page: Click the **Summary** tab
- Click the arrow next to the Messages per page drop-down list, and select the required number of entries to display.

Messages per page: 20 ▾		Displaying 1 - 4 of 4 messages	
Date Received ▾		Size	
6/9/16 10:18 AM		22941	
6/9/16 10:17 AM		3887	
6/9/16 10:17 AM		25554	
6/9/16 10:14 AM		3883	

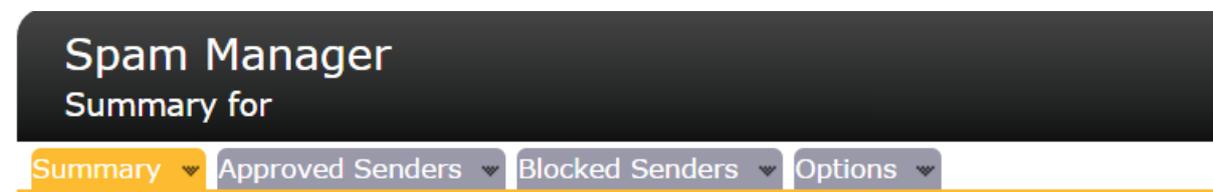
All times are displayed in UTC

Searching for a message

You can search Spam Manager for a message from a specific sender or with a specific subject.

To search for a message:

- Click the **Summary** tab.



You can search for an email by *Sender* or *Subject*. Please enter your search text below.

- Type a keyword (or part of one) to identify the subject line or sender of the email in the search box.

You cannot use wildcards in the search field. For example, if you search for *, you will only find emails that contain the * symbol in the subject line or sender's name.

- Click the **Search** button.

Any messages containing the keyword are displayed.

To list all messages:

- Click the **Summary** tab.
- Click the **Clear Search** button.

All of your messages are listed according to your setting for the number of messages per page.

Selecting messages

When you want to delete or release your messages, you can select them either individually or one page at a time.

To select an individual message:

- Click the **Summary** tab.
- Locate the message and select the checkbox to the left of it.

<input type="checkbox"/>	Sender
<input type="checkbox"/>	↩ mailer@
<input checked="" type="checkbox"/>	mailer@
<input type="checkbox"/>	mailer@
<input type="checkbox"/>	mailer@

To select messages a page at a time:

- Click the **Summary** tab
- Select the checkbox at the top of the list, to the left of the *Sender* column

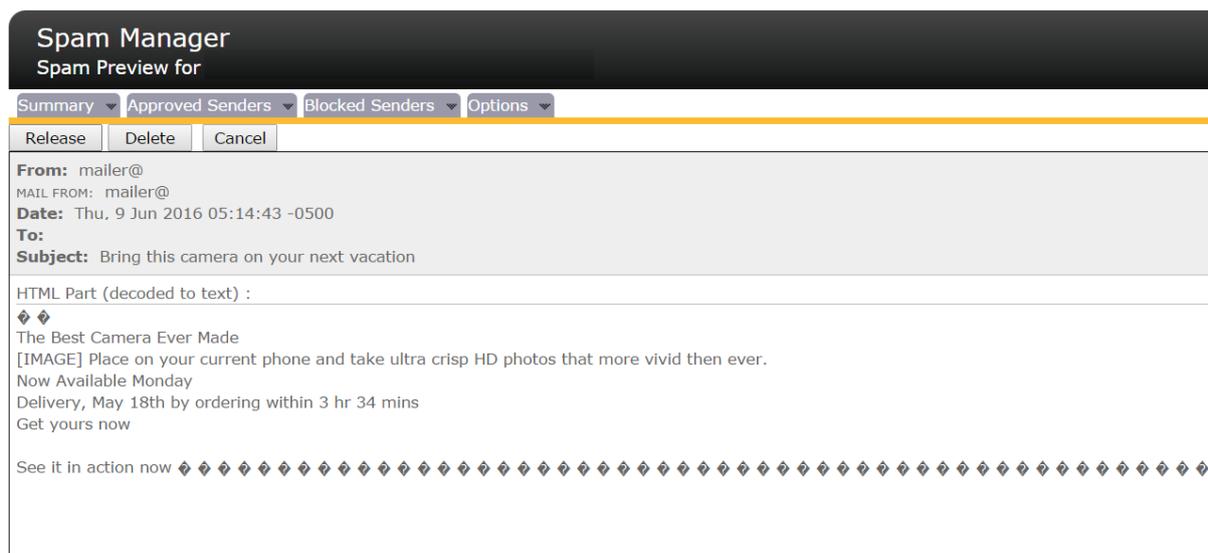
All of the messages on the page are selected.

<input checked="" type="checkbox"/>	Sender
<input checked="" type="checkbox"/>	↩ mailer@
<input checked="" type="checkbox"/>	mailer@
<input checked="" type="checkbox"/>	mailer@
<input checked="" type="checkbox"/>	mailer@

To view the content of a message:

Depending on your organisation's security policy, you may be able to view the text content of the emails displayed in Spam Manager. To do this:

- Click the **Summary** tab.
- Locate the message to view and click on its sender's name. The message is displayed.



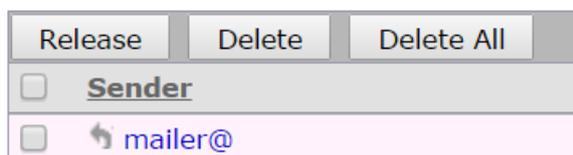
You can check the content of the message and decide whether to release it, delete it, or neither.

If your organisation’s security policy prevents you from viewing the subject or content of email messages in Spam Manager, the only way to be able to read those messages is by releasing them to your email inbox.

You are advised to exercise caution when considering releasing messages with potentially inappropriate content, as once you have released them and received them in your inbox, they become your responsibility.

Releasing messages

When you release a message, it is sent to your email inbox. It remains visible in Spam Manager and can be identified by the small arrow icon next to the subject. Messages can be released individually or a page at a time.

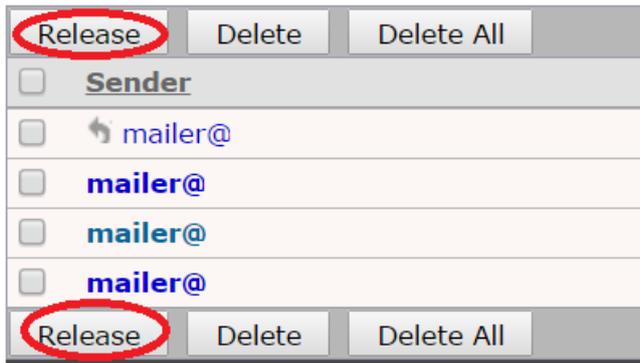


If you are the owner of an account with aliases or an account group and release an email for one of your aliases or member accounts, the email is released to the original recipient’s inbox rather than to your inbox.

To release a message from Spam Manager:

Click the **Summary** tab and either:

- Select the checkbox to the left of the email to release and click the **Release** button at the top or bottom of the list.



- Open the email to release by clicking the sender detail, and click the **Release** button at the top or bottom of the message.

A Message released confirmation message is displayed. You may be able to request that the sender is added to your organisations or your own approved senders list.

To release multiple messages from Spam Manager:

- Click the **Summary** tab
- Select the checkboxes to the left of the emails to release and click the **Release** button at the top or bottom of the list. A **Message released** confirmation message for the first selected message is displayed.
- Click the **Continue** button.

The next Message released confirmation message is displayed. Continue in this way until all of the messages are released.

At each Message released confirmation message, you may be able to request that the sender is added to your organisations or your own approved senders list.

To release a message from an active summary notification:

If your organisation has set up active summary notifications, your summary notifications contain links to release the spam emails without continual logging in to Spam Manager.

You can only release an email, once from an active summary notification due to security reasons. It prevents a malicious user from releasing an email multiple times, thereby performing a denial of service (DOS) attack. If you need to release the email again, you can do so from Spam Manager. Or ask your Quarantine Administrator to release it for you.

From your spam notification email, click the link next to the email you wish to release. The release of the email will be confirmed.

An email cannot be released in the following circumstances:

- The email has already been released via Spam Manager
- The email has already been deleted from Spam Manager, by yourself or a Quarantine Administrator

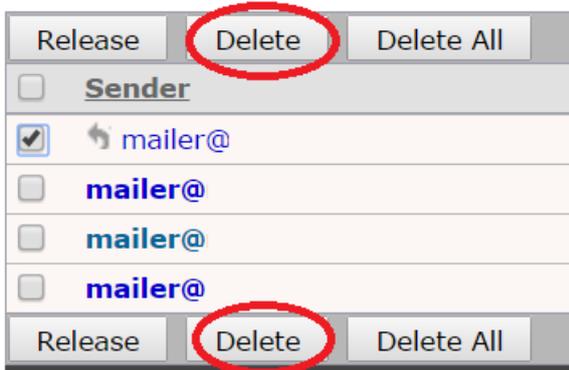
- The email has expired. Spam emails are saved for 14 days.

Deleting messages

When you delete a message, it is removed from Spam Manager. Selected messages can be deleted individually, a page at a time, or all at once.

To delete a message:

- Click the **Summary** tab.
- Select the checkbox to the left of the email to delete and click the **Delete** button at the top or bottom of the list.



Or open the email to delete by clicking the sender detail, and click the **Delete** button at the top or bottom of the message.

To delete a page of messages:

- Click the **Summary** tab.
- Select the checkbox to the left of the sender heading. All of the messages on the page are selected.
- Click the **Delete** button at the top or bottom of the list.

To delete all messages:

- Click the **Summary** tab.

- Click the **Delete All** button at the top or bottom of the list.

