

IBM Express Managed Security Services for Email Security

Anti-Spam Administrator's Guide

Version 5.32

Table of Contents

1. Service overview	3
1.1 Welcome	3
1.2 Anti-Spam (AS) features	3
1.3 How does AS work?	3
1.4 Skeptic heuristic spam detection	4
1.5 Signaturing System	4
1.6 Public blocked senders lists	5
1.7 Custom blocked senders list	5
1.8 Custom approved senders list	5
2. Address Validation	5
2.1 Overview	5
2.2 Registering valid addresses	6
2.3 Address harvesting	6
2.4 Updating registered addresses	6
2.4.1 To upload a list	7
2.4.2 To download the current list	8
2.4.3 To remove items from the current list	8
2.4.4. To add items to the li	9
2.5 Enabling validation	9
2.5.1 To change the current action	10
2.6 Insight roles	10
2.7 Sub-domain addresses	10
3. Anti-Spam service configuration	11
3.1 Overview	11
3.2 Configuring default AS settings	11
4. Configuring custom approved and blocked senders lists	13
4.1 Overview	13
4.2 Validation rules for lists	14
4.3 Manually adding list entries	15
4.4 Downloading a list for offline editing	15
4.5 Uploading a list	16
5. Anti-Spam notification messages	17
6. Anti-Spam statistics	17
6.1 Overview	17
6.2 Viewing AS statistics	17
7. Anti-Spam reports	18
7.1 Overview	18
7.2 AS Report Content	18
7.3 Configuring AS scheduled reports	19
7.4 Spam Quarantine reports	21

1. Service overview

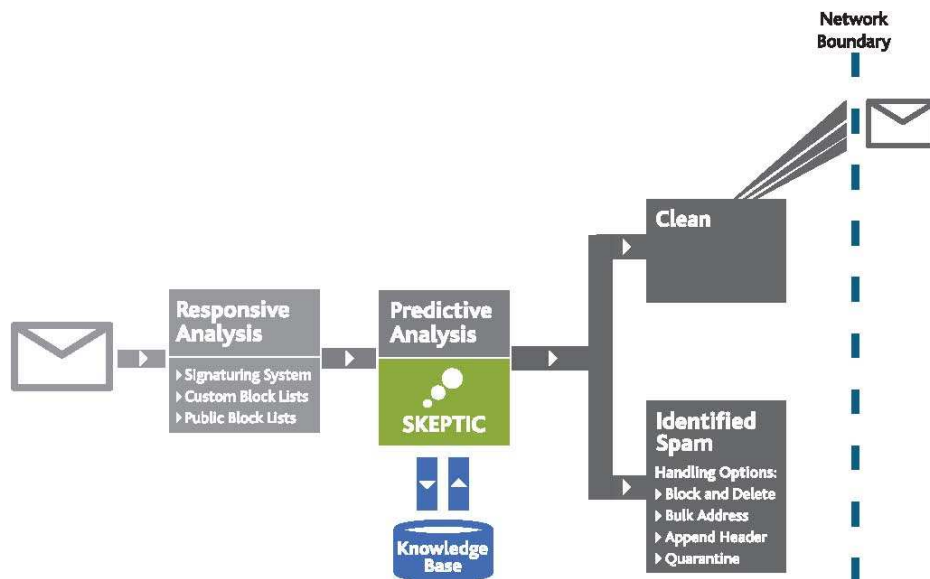
1.1 Welcome

Welcome to the Administrator's Guide for the E-mail Security Anti-Spam service. The following information provides a walk-through of how to set-up the Anti-Spam Service.

1.2 Anti-Spam (AS) features

- Patented Skeptic Heuristics Engine used to block unsolicited commercial email
- Spam signature engines that reduce false positives and increase speed of spam detection
- Detection using public block lists
- Customizable domain, IP and email address blocked and approved sender lists
- Range of actions for each spam detection method.

1.3 How does AS work?



1.3 Anti-Spam Service overview

AS stops unsolicited email from entering your email system. A Skeptic Heuristics Engine, spam signature database, public spam block lists and the custom blocked sender list are used to check all incoming email for spam.

Any domain names, email addresses or IP addresses on the custom allowed senders list will automatically bypass the spam filter.

You can choose which of the AS spam detection methods you require incoming email to be checked against. Either a domain default setting or custom configuration can be applied to each of a client's domains.

If an email is identified as spam, you can choose to apply the following actions to the email:

- Block and delete
- Append a header but allow mail through
- Append a header and redirect to a bulk mail address
- Tag the subject line but allow mail through
- Quarantine the mail (see note below).

All suspected spam is logged within Insight statistics (see [section 5](#)).

Note: Optional Spam Quarantine feature enables you to quarantine detected spam emails. Configuring and using this feature is covered by the Spam Quarantine Administrator's Guide.

1.4 Skeptic heuristic spam detection

Skeptic™ uses artificial intelligence to create an ever-expanding knowledge base for identifying spam. The heuristics method works by scoring each email against a set of rules. If the email in question achieves more than a specified score, it is immediately identified as spam.

1.5 Signaturing System

The Signaturing System leverages both proprietary and commercially available signature-building engines to create a vast knowledge base of samples, or 'fingerprints' of spam messages currently in email circulation. This enables exact matching of spam, significantly reducing chances of False-Positives as well as speeding identification and message handling.

1.6 Public blocked senders lists

The AS service can also scan for email from globally known sources of spam. These are companies and individuals who have demonstrated patterns of junk emailing.

These sources are identified within recognized public block lists of IP addresses. Administrators can opt to use these blocked senders lists through the InSight administration tool.

1.7 Custom blocked senders list

The custom blocked senders list enables you to specify IP addresses of email systems, internet domain names or email addresses which you recognize as sources of spam or other unwanted email.

1.8 Custom approved senders list

Your organization may need to communicate with organizations that appear on a public block list. By adding the relevant IP address, email domain or email address to your approved sender list you can override any public block list entries.

The approved senders list can also be used to ensure that email newsletters, which may occasionally be detected as spam, pass through the spam service without interruption.

2. Address Validation

2.1 Overview

The Email Security Service operates a scheme to protect clients from the increasing prevalence of “dictionary-based” email attacks, commonly associated with spam email. In this form of incident large volumes of email are sent to a very broad range of email addresses within a domain – most of which will be addresses that do not exist and are fabricated by dictionary or algorithmic means.

To protect clients, an “Address Validation” capability is established as an essential part of the Anti-Spam service, which is used to reject any email sent to a client’s domain that does not appear on a database of known valid addresses. For this technique to be effective the client needs to keep the list of valid addresses up to date and to this end a management interface is provided within Insight.

2.2 Registering valid addresses

You will need to compile a list of valid email addresses for each domain that is to be subject to Address Validation. Remember that validation is performed only on the recipient addresses of incoming email to your domains, so you will need to include on this list any alias addresses and externally visible “group” addresses (e.g. sales@domain.com).

Your list of registered addresses can be uploaded via Insight, the file format requirements being:

- a Comma Separated Values (CSV) file
- first field on each line is the address, with one address per line
- any data after the first comma (which is optional) is ignored

The reason for the use of a CSV format is to allow you to maintain a file with additional information against each entry, which can be ignored by the Service for the purposes of address validation.

As the purpose of registering your valid email addresses is to allow us to reject mail to unrecognized addresses, it is important that an up-to-date list is maintained.

2.3 Address harvesting

As an aid to keeping your valid address list current, the Email Security Service will automatically “harvest” the sending email addresses used on email sent from your domains and add these to the list of registered addresses. You will be able to review the result of this harvesting by:

- Downloading the current list
- Interrogating the list via the Edit function

2.4 Updating registered addresses

For each domain, you may choose how you wish to keep your list up to date. It is suggested that you may wish to combine this activity with your existing IS process for handling staff leavers and joiners.

Your options for list management include:

- Periodic refresh of the complete list - achieved by an Upload and Replace operation of your entire list.
Note: this action is recommended at intervals of your choosing to reflect a set of address additions and removals.
- Incremental additions – achieved by an Upload and Merge operation of a list of new addresses.
Note: this action can be used to augment the address harvesting, particularly where new addresses may not be captured by the sending of outbound messages.
- Ad-hoc edits – achieved by an Edit operation.
Note: this action can be used to add or remove individual addresses in between your routine list update cycle.

To manage your list of registered addresses from within Insight:

1. Select **Admin** from the top left-hand menu bar

[STATUS](#) [STATISTICS](#) **ADMIN** [LOG OFF](#)

[Reports](#)

Domains

[Content](#)

[My Profile](#)

Search for Domain:

Change domain options by clicking on the links below.

Domain	Current Settings	Banners & Email Settings	Spam Settings	Image Control Settings	Registered Email Addresses
Defaults	Custom banner on inbound mail.Default banner on outbound mail.	Default Banners & Email Settings...	Default Spam Settings...	Default Image Control Settings...	- - -
radio0.messagelabs.com	Virus Scan using default banner settings.	Banners & Email Settings...	Spam Settings...	Image Control Settings...	Accepting unregistered addresses... Upload... Download... Edit...

Powered by MessageLabs

2.4.1 Manage registered addresses

Select Domains from the top right-hand menu bar.

You will see a column entitled **Registered Email Addresses**. Against each of your domains will be shown the current setting for address validation (where enabled).

2.4.1 To upload a list

Upload Registered Email Addresses For electrum.co.uk

File Name:	<input type="text"/>	<input type="button" value="Browse..."/>
On Upload:	<input checked="" type="radio"/> Delete existing addresses and replace with uploaded addresses <input type="radio"/> Merge existing addresses with uploaded addresses	
Click this button to upload the email addresses file:		<input type="button" value="Upload"/>
Click this button to exit without changes:		<input type="button" value="Cancel"/>

2.4.2 Upload a list

1. Select **Upload...** and a dialog box will be presented.
2. Specify, or **Browse** for, the source file on your local system that holds your list of addresses.
3. Select **Delete existing addresses** if you wish to replace the current list with the uploaded list
OR
Select **Merge existing addresses** if you wish the new list to be merged with the current list (all duplicate entries will be ignored).
4. Select **Upload** button to start the upload operation.

Note: the upload operation may take some time to complete depending on the size of list.

2.4.2 To download the current list

1. Select **Download...** and a dialog box will be presented
2. Specify, or **Browse** for, the target file on your local system that will hold your list of addresses
3. Select **Download** button to start the download operation

Note: the download operation may take some time to complete depending on the size of the list.

2.4.3 To remove items from the current list

Edit Registered Email Addresses For electrum.co.uk

(Use * as a wildcard)

Email		
1@electrum.co.uk	Edit	Delete
10@electrum.co.uk	Edit	Delete
100@electrum.co.uk	Edit	Delete
11@electrum.co.uk	Edit	Delete
12@electrum.co.uk	Edit	Delete
13@electrum.co.uk	Edit	Delete
14@electrum.co.uk	Edit	Delete
15@electrum.co.uk	Edit	Delete
16@electrum.co.uk	Edit	Delete
17@electrum.co.uk	Edit	Delete

1 2 3 4 5 All

Displaying 1 to 10 of first 50 (100 total)

Add Entry

Add a single entry:

Click this button to update the email addresses:

Click this button to exit without changes:

2.4.3 Edit dialog box

1. Select **Edit...** and a dialog box will be presented
2. Specify the address to be removed in the text box (the * wildcard may be used for partial matching)
3. Select the **Search** button
4. Locate the entries you wish to delete – you may need to page through the results
5. Select **Delete** for each entry that you wish to remove (you may also select **Edit** to change an existing entry)
6. Select the **Update** button to complete the operation and save the changes

2.4.4. To add items to the list

1. Select **Edit...**
2. Select the **Add Entry** button and enter the required address
3. Select the **Update** button to complete the operation and save the changes

Note: any change to list content will be subject to the normal configuration update cycle.

2.5 Enabling validation

By default, when address validation is made available to you the system will continue to accept email from invalid addresses until such time as you have established your list and wish to switch the validation action to Reject. Once the action for a domain is set to **Reject** then any email sent to an unregistered address will not be accepted and will give rise to an SMTP 550 error, which indicates to the sending mail server that the address is invalid.

2.5.1 To change the current action

Registered Email Addresses - electrum.co.uk

On Receiving Incoming mail to Unregistered Email Addresses:

Action:

Click this button to update:

Click this button to exit without changes:

2.5 Action setting dialog box

1. Select whichever of “**Accepting**” or “**Rejecting**” is showing and a dialog box will be presented
2. Change the **Action** to be either **Accept** to switch off address validation
OR
Change the **Action** to **Reject** to apply address validation using your current list of registered addresses
WARNING: Do not set “Reject” unless you have put in place the list of registered addresses that you wish validated. Failure to do this may cause email to valid addresses to be rejected.
3. Select **Update Settings** to complete the operation and save the changes

Note: any change of action, such as switching **Accept** to **Reject**, will be subject to the normal configuration update cycle.

2.6 Insight roles

For an Insight user to view and edit the address validation functionality they require the following roles:

- Mail Management – “Edit Configuration” and “View Configuration”
- Anti-Virus - “Edit Configuration” and “View Configuration”

For more information on Insight user roles refer to the Insight Administrator’s Guide, section 4.

2.7 Sub-domain addresses

If you have email addresses that exist on sub-domains (e.g. user@sub.domain.com) then these addresses should not be included in the valid address list for domain.com. Instead you should do one of the following:

- If you wish for address validation to be performed for addresses on sub-domains, then each sub-domain should be provisioned separately so that an appropriate address validation list can then be provided.
- If you do not wish for address validation to be performed for addresses on those sub-domains, then you need take no further action (but please remember **not** to

include these sub-domain address in any other address validation lists).

3. Anti-Spam service configuration

3.1 Overview

AS is configured in two steps:

1. Configure the Default Anti-Spam settings. This entails:
 - Selecting spam detection methods and lists
 - Defining actions to be taken on detection of spam
 - Setting the AS bulk-mail address to where spam email will be routed if spam email redirection is selected.
2. Configure approved and blocked sender list entries.

Note: the spam service is not automatically enabled when the service is purchased. You must activate the different spam detection methods to enable the service.

3.2 Configuring default AS settings

1. Log in to InSight
2. Select **ADMIN** from the top-left menu bar
3. Select **Domains** from the top-right menu bar
4. Select **Default Spam Settings**
5. The following screen will appear:

Anti Spam Settings for Client

Config
Approved senders
Blocked senders

Bulk Mail Address:	Enter one address: <input style="width: 80%;" type="text" value="spam@yourdomain.com"/> <small>(Leave blank if unknown)</small>
Subject tag text:	Enter text for subject line tagging: <input style="width: 80%;" type="text" value="SPAM:"/> <input checked="" type="radio"/> prefix subject <input type="radio"/> append to subject
Approved Senders List:	<input checked="" type="checkbox"/> Use Custom IP Approved Senders List <input checked="" type="checkbox"/> Use Custom Domain Approved Senders List
Responsive technologies	
Blocked Senders list (IP)	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Block and delete the mail"/>
Blocked Senders list (Domain)	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Block and delete the mail"/>
Public Block list (ORDB)	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Append a header and redirect to a bulk mail address"/>
Public Block list (RBL)	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Append a header but allow mail through"/>
Public Block list (RSS)	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Append a header but allow mail through"/>
Public Block list (DUL)	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Append a header but allow mail through"/>
Signaturing system	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Block and delete the mail"/>
Predictive technologies	
Skeptic Heuristics	<input checked="" type="checkbox"/> Use on detection: <input style="width: 80%;" type="text" value="Block and delete the mail"/>

Click this button to update these settings:
Click this button to exit without changes:

3.2 Configuring default Anti-Spam settings

The options available are:

1. **Bulk Mail Address:** specifies 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
2. **Subject tag text:** specifies the text that is prefixed or appended to the subject line of a suspected spam email when the **Tag the subject line but allow mail through** action is selected. The default action is to prefix 'SPAM:' to the subject line
3. **Approved senders list:** select whether to enable the approved senders IP or domain lists. The domain list also covers approved email addresses
4. **Responsive technologies:** use existing information on known spammers, spam email signatures and the custom blocked senders list
 - a. **Blocked Senders list (IP) & Blocked Senders list (Domain):** select whether to enable the blocked senders IP or domain lists. The domain list also covers blocked email addresses
 - b. **Public Block list ORDB:** use ORDB (Open Relay Database) public block list
 - c. **Public Block list RBL:** use RBL (Real Time Blackhole List) public block list

- d. **Public Block list RSS:** use RSS (Relay Spam Stopper) public block list
 - e. **Public Block list DUL:** use DUL (Dynamic User List) public block list
 - f. **Signaturing System:** use the comprehensive database of known spam signatures
5. **Predictive technologies:** use heuristic technologies to identify new spam according to known spam characteristics.

Select either the default or custom Anti-Spam settings for each domain. Initially all domains are set to the default settings. To define custom settings select the **Spam Settings** option next to the relevant domain name.

You can choose to deal with suspected spam as follows:

1. Block and delete the email
2. Append a header but allow the email through
3. Append a header and redirect to the defined bulk-mail address
4. Tag the subject line but allow the email through
5. Quarantine the mail (see note below).

The **'append a header'** part of the action adds a string to the internet email header. The format for the string is 'X-Spam-Flag: YES'. This string identifies the email as spam, enabling further action when it enters the client's mail system or an end users' email client. For example diversion of the email into a 'spam' folder.

Note:

- By default all spam detection methods are disabled
- Only one bulk-mail address can be set up for each domain and this is used by all the detection methods enabled for that domain
- Links are provided to the web sites of the public block list providers (click on their name)
- Optional Spam Quarantine feature enables you to quarantine detected spam emails. Configuring and using this feature is covered by the Spam Quarantine Administrator's Guide.

4. Configuring custom approved and blocked senders lists

4.1 Overview

Custom approved and blocked senders lists provide a simple way for administrators to indicate sets of emails that should always be allowed through or blocked from inbound

email.

There is only one approved sender list and one blocked sender list per client. Administrators can define whether specific domains use these lists or not.

The same management interface is used for both the approved and blocked sender lists so you can use the following instructions for both list types. Lists can be downloaded for offline editing and uploaded back into InSight.

Locating the approved and blocked sender lists

1. Log in to InSight
2. Select **ADMIN** from the top-left menu bar
3. Select **Domains** from the top-right menu bar
4. Select **Edit Default Spam Settings**
5. Select the **Approved senders or Blocked senders** tab.

Anti Spam Settings for Client

Config | **Approved Senders** | Blocked senders

All Emails Domains IPs Search (Use * as a wildcard)

Email, Domain or IP	Description	Edit	Delete
123.123.123.123	Server 3	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
124.234.23.111	Server 2	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
125.235.16.12	VP 11-03	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
abc.com	requested by the VP on 12-3-03	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
domainname.com	test	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
ft.com	Financial Times	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
good.people.net	Good people	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
goodguy@domain.com	This is a good guy	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
hotmail.com	Staff use	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
innesfarm.com	Rural retreat	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1 2 3 All

Displaying 1 to 10 of 27

A whole IP Address class C block may be matched using a wildcard, e.g. 192.168.0.*.

Add Entry **Upload** File: **Download** Download entries to file:

Action: Replace Merge

Add entries from file:

Click this button to update these settings:
Click this button to exit without changes:

4.1 Example Anti-Spam approved senders list

4.2 Validation rules for lists

The following rules apply to all approved and blocked sender list entries:

- **Email address** – full email addresses with valid domain names are accepted, e.g., 'broberts@shopping.com'. Partial email addresses, such as 'broberts@shopping', are not valid
- **Domain name** – full domain names, such as 'xxx.yyy.com', are accepted. Top-level domains (e.g. 'com' or 'uk') or partial domains with the top-level domain present (e.g. 'yyy.com') are also valid. Partial domains without the top-level domain (e.g. 'xxx' or 'yyy') are not valid. The '*' wildcard is also not valid within a

domain name

- **IP address** – a series of basic IP address validation rules are used within InSight to prevent any invalid IP addresses being entered into the spam lists. It is still possible to use the “*” wildcard to match a whole IP address class C block e.g. ‘192.168.0.*’.

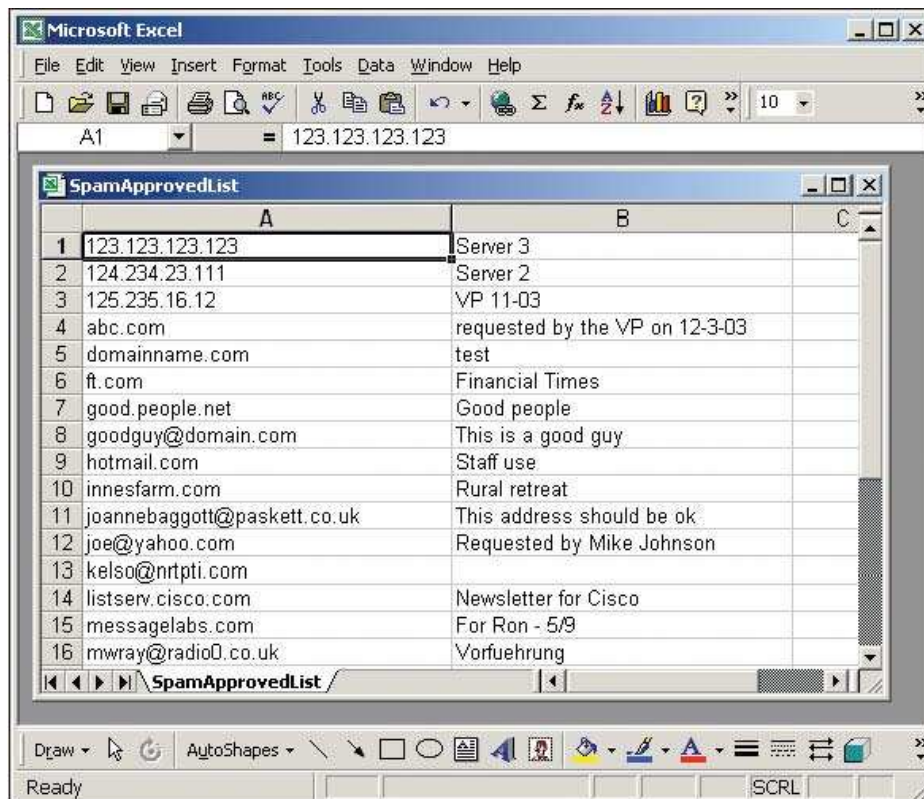
4.3 Manually adding list entries

1. Select **Add Entry**
2. Enter the email address, domain name or IP address, and entry description
3. To commit the entry into the list select **Update**
4. It is possible to cancel the addition of the new entry by selecting **Cancel**.

4.4 Downloading a list for offline editing

1. Select **Download**
2. Select the location to save the list
3. The file will be automatically named **SpamApprovedList.csv** or **SpamBlockList.csv**

The following screenshot shows the content of an approved senders list within Excel:



4.4 Downloading a list for offline editing

The first column lists the IP, email address or domain entry and the second column lists associated descriptions.

Existing entries can now be edited and new entries can be inserted into the list. When saving the list ensure that it is saved using CSV (comma delimited) or Text (tab delimited) format.

4.5 Uploading a list

You have two options available for uploading lists into InSight:

1. **Replace** – by selecting this option the uploaded list will replace the existing list.

Note: Any entries in the existing list that are not in the uploaded list will be lost

2. **Merge** – by selecting this option the uploaded list will merge into the existing InSight list. This is a useful way to add new entries to an existing list.

Note: When merging, if duplicate IP, email addresses or domain entries exist within both the uploaded and existing list InSight will highlight the number of duplicates and provide you with the option to overwrite the entries in the existing list (potentially changing their description) or cancel the list merge process.

To upload a list:

1. Select **Browse** and locate the list file
2. Select either **Replace or Merge** action and then **Upload**
3. New list entries will be added into the list displayed within the browser.

Note: changes to the lists will not be passed onto the Anti-Spam Service until the **Update** button at the bottom right of the screen has been selected. It can then take up to 24 hours for the changes to become active.

5. Anti-Spam notification messages

By design there are no notifications for Anti-Spam.

6. Anti-Spam statistics

6.1 Overview

The Spam Statistics page displays the volumes of suspected spam detected, broken down by detection type.

6.2 Viewing AS statistics

1. Log in to InSight
2. Select **STATISTICS** from the top-left menu bar
3. Select **Spam** from the top-right menu bar
4. Select the period for which you want statistics, i.e. Day, Week, Month or Year.
5. Select a Detected By type within the AS statistics screen to display a detailed list of the spam emails detected by the chosen detection type.

Details provided are:

- Date/Time
- Recipient
- Sender
- Subject
- Detected By
- Sender IP.

Insight Account Management - Microsoft Internet Explorer

File Edit View Favorites Tools Help

STATUS STATISTICS ADMIN LOG OFF

Email Virus Spam Image Content

Day | Week | Month | Year

Viewing spam statistics for the last 7 days.

	Number Of Messages	% of Total Mail	% of Total Spam
Total Emails	3260157	100	0
Detected By Signaturing system	1056594	32.41	57.25
Detected By DUL	595425	18.26	32.26
Detected By Skeptic Heuristics	125575	3.85	6.80
Detected By RBL	61448	1.88	3.33
Detected By RSS	4306	0.13	0.23
Detected By IP Blocked List	1119	0.03	0.06
Detected By Domain Blocked List	1051	0.03	0.06
Detected By ORDB	0	0	0
Total Detected Spam	1845518	56.61	100

Powered by MessageLabs

Done Internet

Note: only the first 150 spam statistics are shown.

7. Anti-Spam reports

7.1 Overview

Reports of AS activity are automatically emailed to a specified address on a weekly or monthly basis. You can configure the recipient email address and the frequency for distribution of reports to your specified address.

7.2 AS Report Content

- **Weekly and Monthly summary report** - a set of tables that provide an overview of key statistics for the AS service for the specified period across all client domains.
- **Service summary for all domains** (mail volume, spam volume, spam volume as a percentage of total mail, spam volume for each type of detection and as a percentage of total spam and total mail)
- **Service summary by domain** (domain name, mail volume, spam volume and spam volume as a percentage of total mail)
- **Top 100 spam sources by domain** (domain name, spam volume).
Note: this is an optional report table.
- **Top 100 spam sources by IP** (IP address, spam volume).
Note: this is an optional report table.
- **Top 50 recipients of spam** (recipient email address, spam volume).
Note: this is an optional report table.

Note: Due to the large volume of spam processed it is no longer feasible to produce a detailed Anti Spam report that can be emailed to clients. If you have a specific requirement for this information then please contact your client service representative.

7.3 Configuring AS scheduled reports

Configuring reports

1. Log in to InSight
2. Select **ADMIN** from the top-left menu bar
3. Select **Reports** from the top-right menu

The screenshot shows the InSight interface with the top navigation bar containing **STATUS**, **STATISTICS**, **ADMIN**, and **LOG OFF**. Below this, a secondary navigation bar includes **Reports** (highlighted in orange), **Domains**, **Content**, and **My Profile**. A message reads: "View reporting options by clicking on a service below." Below this is a table with three columns: **Service**, **Reports**, and **Recipients**.

Service	Reports	Recipients
Anti-Virus	Weekly Summary Report (Text) Weekly Detail Report (Text)	av-reports@messagelabs.com cwyss@ggs.ch colman@colman.com colman1@colman.com cocolman@colman.com colman2@colman.com
Anti-Spam	Weekly Summary Report (Text) Monthly Summary Report (Text)	admin@messagelabs.com testagain@update.com
Spam Quarantine	Weekly Summary Report (HTML)	test@messagelabs.be test@messagelabs.com
Image Control	Monthly Summary Report (Text)	admin1@messagelabs.com
Content Control	Monthly Summary Report (Text)	test2@messagelabs.com

Powered by MessageLabs

7.3 Reports Overview

3. You can now see an overview of the current Reporting settings. The **Reports** column lists currently subscribed to reports and the **Recipients** column the email addresses that will receive those reports.
4. Select **Anti-Spam** from the **Service** column
5. A pop-up window will appear containing the report settings for the AS service.

Anti-Spam Report Settings for Client

Recipients:	admin@eg.com monitor@eg.com	Edit Edit	Delete Delete
Click this button to add a new email address: <input type="button" value="Add"/>			
Reports:	Format	Elements	
Weekly Summary	<input type="text" value="Text"/>	Expand >>	
Weekly Detail	<input type="text" value="CSV"/>	Expand >>	
Monthly Summary	<input type="text" value="Text"/>	Expand >>	
Click this button to update these settings: <input type="button" value="Update"/>			
Click this button to exit without changes: <input type="button" value="Cancel"/>			

- Report recipients can be added, edited or removed within the **Recipients** row.
- The **Reports** row enables you to specify which reports to receive and also the format each report is delivered in. By default the **Format** drop down is set to **None** for each report type. Selecting either **Text** or **CSV** from the drop down list activates the report.
- Content of reports can be defined by clicking on the **Expand>>** text under the **Elements** column.

Anti-Spam Report Settings for Client

Recipients:	admin@eg.com monitor@eg.com	Edit Edit	Delete Delete
Click this button to add a new email address: <input type="button" value="Add"/>			
Reports:	Format	Elements	
Weekly Summary	<input type="text" value="Text"/>	<< Collapse	
<input type="checkbox"/> Total for all domains <input checked="" type="checkbox"/> Total by domain <input type="checkbox"/> Top 100 spam sources by domain <input type="checkbox"/> Top 100 spam sources by IP <input type="checkbox"/> Top 50 recipients of spam			
Monthly Summary	<input type="text" value="Text"/>	Expand >>	
Click this button to update these settings: <input type="button" value="Update"/>			
Click this button to exit without changes: <input type="button" value="Cancel"/>			

- Certain report elements are mandatory (grayed out ticks) but others can be selected by ticking the relevant element box.
- To update your report settings click on the **Update** button.

7.4 Spam Quarantine reports

If you use the Spam Quarantine functionality there a set of additional reports available to monitor the quarantine service. These weekly or monthly reports provide a summary of email releases from the quarantine and also logons to Spam Manager. A report is sent for each domain configured for the Spam Quarantine.

The reports are currently only available in HTML format. They are configured and requested in the same manner as the standard Anti-Spam service reports.

Spam Quarantine Report Settings for Client			
Recipients:	No email addresses		
	Click this button to add a new email address: <input type="button" value="Add"/>		
Reports:		Format	Elements
	Weekly Summary	<input type="text" value="None"/>	<< Collapse
		Quarantine releases per domain	<input checked="" type="checkbox"/>
		Quarantine logins per domain	<input checked="" type="checkbox"/>
	Monthly Summary	<input type="text" value="None"/>	Expand >>
	Click this button to update these settings: <input type="button" value="Update"/>		
	Click this button to exit without changes: <input type="button" value="Cancel"/>		