IceWarp Unified Communications

AntiSpam Reference

Version 12.0

Published on 3/8/2018

Contents

Anti-Spam 5

About 6
New Internal Processing 6
Hits and SpamAssassin Score Separated 6
Smarter Behavior of Address Book Whitelists 6
New Spam Reports 6
Distributed Domains 6
Reference 7
General 7
General 7
Other 8
Action 11
Action 11
Tuning Default AntiSpam Limits 13
Reports 13
How to Set Anti-Spam Reports 15
Different Report Schedules 17
Quarantine 19
Quarantine Report 21
Processing for Incoming Messages 21
Processing for Pending Queue 22
Challenge Response – How It Works 23
Screenshot Examples 24
SpamAssassin 25
SpamAssassin – RBL 28
IceWarp Anti-Spam LIVE 29
IceWarp Anti-Spam LIVE Classifications 31
Reporting False Classifications 32
Email Address to Report To 33
Bayesian 33
Bayesian Filters – Basic Explanation 34
spam.db and spam.usr Files 35
Black & White Lists 35
Blacklist 35
Whitelist 36

Greylisting 38
Greylisting Flowchart 40
Learning Rules 41
Miscellaneous 43
Content 43
Charsets 44
Senders 44
Spam Scores Concept 45
Rules Customization – local.cf File 46
Spam Queues 47
Logging 48
Reason Codes 50
AntiSpam Flowchart 52

Anti-Spam

IceWarp Server integrates many Anti-Spam technologies to protect your users from spam.

IceWarp Server uses SpamAssassin, Bayesian Filters, Greylisting, Razor and Content Filters, giving you one of the most comprehensive present-day AntiSpam tool set.

Whether a message is marked as spam or not is based on a score, up to 10. All of the Anti-Spam technologies modify this score according to their findings. At the end of the whole process, IceWarp Server checks the spam score and acts accordingly. You have control over what spam score causes a message be classified as spam, quarantined, or deleted.

Legend

Icon	Description
	Warning – very important!
	Note or tip – good to know.
NOTE: Areas...	*Note within a table.*
▸ Figure 4	Figure link – click the link to reveal the figure. Click it again to close it. (Works only in the ***CHM*** format.)

Registered Trademarks

iPhone, iPad, Mac, OS X are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft, Windows, Outlook and Windows Phone are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Android is a trademark of Google Inc. IceWarp is a registered trademark in the USA and other countries.

About

New Internal Processing

Redesigned and documented. Solves any problems and downsides of bypasses, access modes, multiple recipients issues, content filter collisions and more.

Hits and SpamAssassin Score Separated

Anti-Spam hits and SpamAssassin score are now two separate values, logged independently in logs and header reports, to allow easier analysis and fine tuning.

Smarter Behavior of Address Book Whitelists

Increased protection from emails with forged ***From*** through **Mail Service – Security – General – *Reject if originator's domain is local and not authorized.*** Now checks both ***From*** and the ***From header*** and in case either of these contains local, non-authenticated recipient, it skips all whitelists and bypasses (DB whitelist, IM roster whitelist). If ***SpamSkipBypassLocalUntrusted*** option (enabled by default) takes action, whitelist is skipped even if message should be quarantined.

New Spam Reports

DB driven, new Quarantine API, new scripts, automatic engine URL, single user/domain/ domain alias support, speed, performance and memory optimizations, handles thousands of accounts, adds logging. System URI's were updated from /challenge/ to /reports/.

Distributed Domains

Anti-Spam is not performed for external recipients of distributed domains, this can be disabled by API variable **C_AS_BypassDistributedDomain** (set to *false*). If disabled, Anti-Spam is performed provided that it is set for ***outgoing messages***.

Learning Rules – EML Support

Also ***.eml*** files sent to learning rule accounts are processed accordingly.

Extended Logging

See the real recipient action, multiple recipient messages logged separately.

Asian Bayes

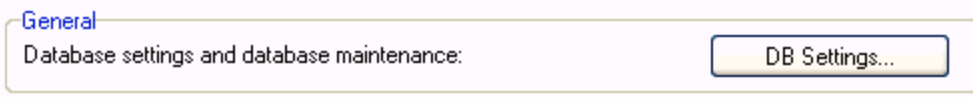
Optimized for handling Chinese, requires teaching, Asian SpamAssassin recommended.

Reference

This chapter describes the **Anti-Spam** node of the IceWarp Server administrative console.

General

General



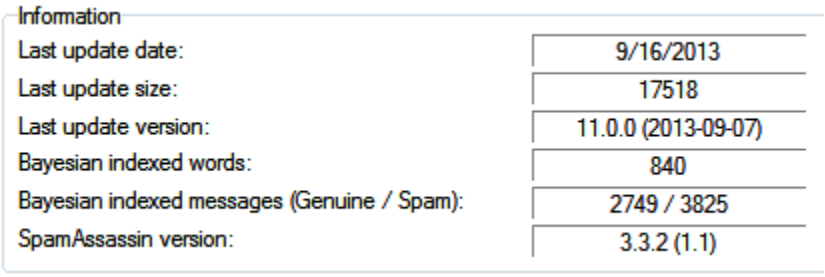
Field	Description
Database settings and database maintenance	Click the ***DB Settings*** button to modify database settings. (See the **Database Settings** section for more details.) By default, IceWarp Server installs with an ***SQ Lite*** database to store data. You should be aware that MS Access can become severely slow when the database contains more than 10K records and at this point you should consider moving to an industrial-strength database.

Access mode to the service can be set on both domain and user levels. See the appropriate places (**[domain] – Policies**, **[user] – Policies**).

The ***Updates Schedule*** section allows you to schedule hands-free updates to the Anti-Spam Reference Base, which is used by the Bayesian filters for accurate spam recognition.

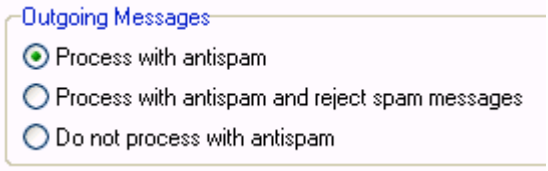
*NOTE: Server-based indexing (see **AS Bayesian**) creates a separate user Reference Base.*

Field	Description
Enable	Check this box to enable automatic updates of the Reference Base.
At:	Specify time when the update is to be done.
Su – Sa	Check the days when the update is to be done.
Update Now	Click this button to update the Reference Base immediately, if required.



Field	Description
Last update date	The date when the Reference Base was last updated.
Last update size	Shows the size of the last update file (in Bytes). Can be useful for troubleshooting.
Last update version	Shows which version of the Reference Base is in use.
Bayesian indexed words	Shows the number of words in the Bayesian database.
Bayesian indexed messages (Genuine/Spam)	Shows the number of genuine and spam messages that have been analyzed to produce the Bayesian database.
SpamAssassin version	Shows which version of the SpamAssassin engine is running.

Other

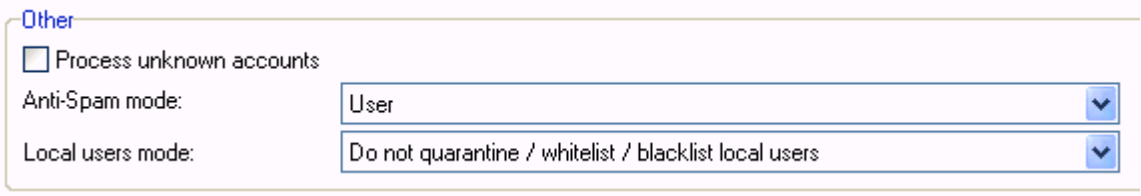


These options allow you to define what anti-spam processing will be performed on outgoing messages.

Choose from the options listed:

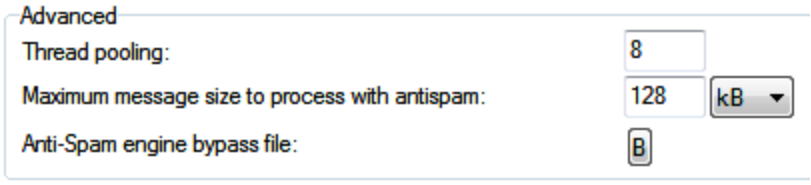
Field	Description
Process with antispam	Use this option to have all messages processed but then forwarded no matter what the result. Messages identified as spam will be marked according to your settings and sent.
Process with antispam and reject spam messages	Use this option to have all messages processed and any that are identified as spam will be rejected.
Do not process with antispam	Use this option to bypass anti-spam processing. You should only use this if you trust all users on your system. **Example**: Processing Mailing list as External Delivery. In case that you want to disable the Anti-Spam filter for mailing lists, you have to **enable** the external delivery for all mailing lists on the server. Mailing lists will be processed as outbound. **tool --filter="(u_type='1')" set account @ m_deliverexternally 1** The anti-spam settings is set to "not process with anti-spam (outgoing messages)".

	Now if you send email to mailing list, then mailing list will be not processed by AntiSpam.



Field	Description
Process unknown accounts	This option tells IceWarp Server what to do when a message comes in for an undefined account (for example a message that is going to be forwarded to a defined account via rules). Check the box to have these messages processed by the anti-spam engine.
Anti-Spam mode	Choose from one of the following: **User** The email address is added to the recipient's whitelist. This mode is best for ISP's whose customer base within a domain are unrelated. **Domain** The email address is added to the whitelist of the recipient's domain. This mode is best for ISP's that host multiple "company" domains, where all domain users are related somehow. **System** The email address is added to the whitelist for the whole IceWarp Server installation. This mode is best for company installations of IceWarp Server. *NOTE: Setting the anti-spam mode to **Domain** or **System** can make the blacklist and whitelist records appear confusing as they have specific user accounts specified as owners of records. This can cause some confusion if another user is questioning why a message did, or did not, get through.* *For example: When you change the mode from **User** to **Domain**, all whitelist/blacklist entries of individual users will apply to the whole domain. Vice versa, when changing the mode to **User**, whitelist/blacklist entries will apply only to their owners.* *NOTE: This setting has influence on a database "level" that is used for address whitelisting when the **Auto whitelist trusted email recipients to database** box is checked.* For more information about whitelisting, auto-whitelisting and whitelist clearing, refer to the **AS – Whitelist** chapter.
Local users mode	Select one of the three options defining how you wish to process messages from other users on the same server (but maybe in different domains). **Do not quarantine / whitelist / blacklist local users** Users from domains on this server will not be challenged. Use this if you trust all users in all domains. **Quarantine / whitelist / blacklist all local users** All users will be challenged. Use this if you host any domain(s) of un-trusted, unrelated users. **Quarantine / whitelist / blacklist local users from other domains** Local users will be challenged if they are from a different domain on the server.

	Use this if you host domains of trusted and un-trusted users (e.g. corporate domains).



Field	Description
Thread pooling	Specify here the maximum number of threads to use when processing messages with the anti-spam engine. *This can be useful for reducing (or increasing) server load.*
Maximum message size to process with antispam	Specify a maximum size of message to be processed with the anti-spam engine.
AntiSpam engine bypass file	Click the **B** button to open the **Bypass** file, listing any users, accounts or domains from which messages will not undergo anti-spam processing. The **Bypass** dialog opens. For more information about this dialog, refer to the **Bypassing Rules/Filters** chapter.

*NOTE: You can get comprehensive spamassassin rule statistics by specifying a file name in the settings file. Do this under the **spamassassinrulestats** entry in the format:*

spamassassinrulestats="<filename>"

You can use date/time variables here if you want to create daily/hourly files etc.

spamassassinrulestats="yyyymmddhhnnss.txt"

The contents of the files will allow you to see which rules have been used and how many times and also you can analyze which rules have ***not*** been hit, allowing you to delete them to speed up processing and save processing power of your server. A simple example from a statistics file is shown below:

SpamAssassin statistics 2007-08-15 00:00

Genuine: 649

SpamQuarantine: 0

SpamMarked: 416

SpamRefused: 205

SpamAssassin: 481

Rules: 1293

Hits: 254

TotalHits: 13588

NoHits: 1039

Rules with hits:

__FRAUD_DBI (1.00) 29

.... list of rules

Total: 254, Hits: 13588

Rules with no hits:

DRUGS_DEPR_EREC (1.00) # Refers to both an erectile and an antidepressant ... list of rules

Total: 1039

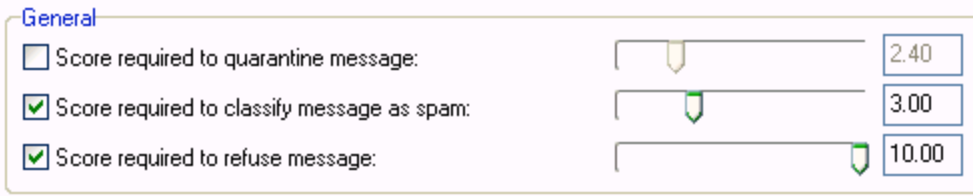
Action

Action

The **Action** tab allows you to define what actions should be taken according to the Spam score.

You should be aware that the spam score is always a value from 0 to 10, with 10 signifying the highest probability that the message is spam.

A score of 0 is assigned to a message if it bypasses spam processing.



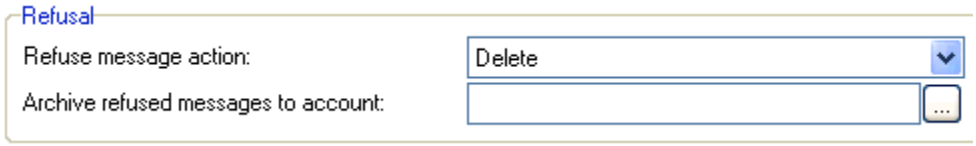
Field	Description
Score required to quarantine message	Check this option to have a message quarantined if its spam score equals to or is higher than the value selected. Move the slider to change the value. *NOTE: The **Quarantine** function must be enabled for this control to work.*
Score required to classify message as spam	Check this option to have a message classified as spam if its spam score equals to or is higher than the value selected. Move the slider to change the value.
Score required to refuse message	Check this option to have a message deleted/rejected (see further) if its spam score equals to or is higher than the value selected. Move the slider to change the value.

NOTE: Quarantined messages are held in a pending queue until they are authorized, manually delivered, or deleted.

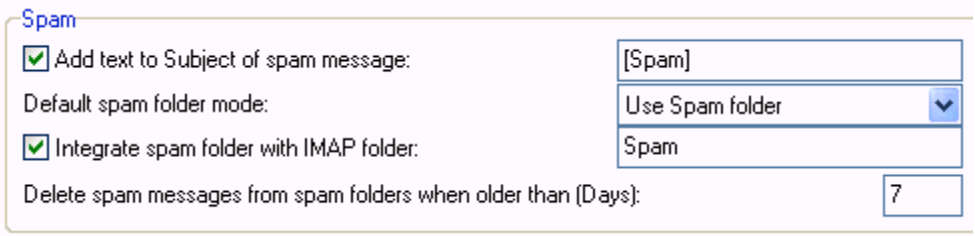
*Authorization is either manual, by a user or domain administrator using WebAdmin or IceWarp WebClient, or automatic if the sender responds to a Challenge Response email (see **AntiSpam – Quarantine**).*

*Deletion is either manual, by a user or domain administrator using WebAdmin or IceWarp WebClient, or automatic if set within IceWarp Server (see **AntiSpam – Quarantine**).*

Manual delivery can only be done by a user or domain administrator using IceWarp WebClient or WebAdmin.



Field	Description
Refuse message action	Select an action for messages that are refused. **Delete** Choosing this option causes IceWarp Server "deletes" the message without informing the sending server, so the sender does not get information about it. **Reject** Choosing this option causes IceWarp Server rejects the message and sends an informational message to the sending server.
Archive refused messages to account	Select an account to have refused messages archived to. Use the '...' button to open the **Select Item** dialog. This option works whether the ***Delete*** or ***Reject*** option (above) is chosen.



Field	Description
Add text to Subject of spam message	Check this option to have text added to the subject of messages classified as spam. Specify the required text in the text box. Note that server variables can be used in this field. Example: You have a spam message with the following subject: *Cheap Meds Here* You can define this text: *[Spam %%SpamScore%%]* The user will receive a message with this subject: *[Spam 5.97] Cheap Meds Here* (If this score identifies the message as a spam.) This lets your users define rules in their email clients to deal with suspected spam messages.
Default spam folder mode	Select whether users will have the **Spam** folders enabled. ▪ ***Use Spam folder*** Messages marked as a spam will not be saved to the user's Inbox, but will be saved to a separate spam folder. You can further define spam administrator(s) who can maintain one or more spam folders. This can be a great time-saver for busy executives, allowing an assistant to check the **Spam** folder for any "real" messages and moving them accordingly. ▪ ***Do not use Spam folder*** All messages – both spam and non-spam ones will be saved in the **Inbox** folders. *NOTE: Users who do not use spam folders does not see them in IMAP (nor in WebClient).* *There are two ways how to disable use of a spam folder for particular user:*

	1) ***User settings – Options – Spam folder mode*** *= disabled (****Do not use Spam folder****)* *2)* ***User settings – Options – Spam folder mode*** *= default,* ***Antispam – Action – Place spam messages under spam folders*** *= disabled*
Integrate spam folder with IMAP folder	Check this option to have the **Spam** folder integrated with your IMAP accounts. Enter the name of the IMAP folder to be used for spam.
Delete spam messages from spam folders when older than (Days)	Specify a number of days after which messages are automatically deleted from the **Spam** folder.

Tuning Default AntiSpam Limits

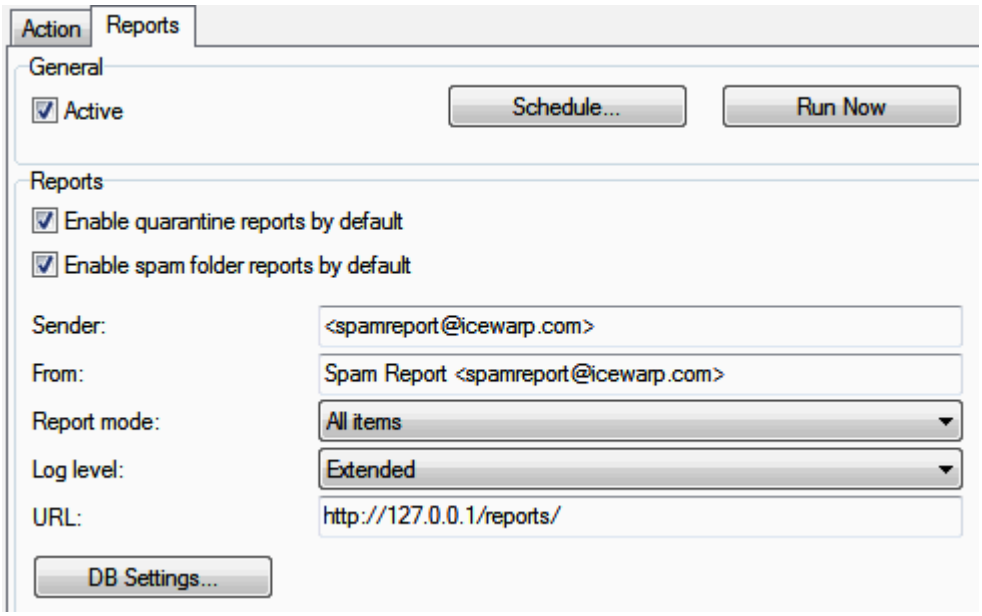
Besides limits set in the console, you can use the API console to set other limits via API variables:

c_as_spammaxtextbyte (default 4096 B) – increase this value to protect from spam that has small amount of text and a lot of images. This value works as a size of buffer for evaluation of regex based rules, so should be adjusted with caution, or the regex parser will run out of stack space.

c_as_ignorefileslarger (default 128 kB) – the message limit should be increased with caution up to 512 kB. You can put more on systems which have a low AntiSpam load or where most of emails are being whitelisted.

c_as_live_ignorefileslarger (default 25 MB) – increase only if you have a default setting in the **Action** tab i.e. LIVE is only scanning small part of incoming messages, but typically it is good enough if you have already set mail limit to 10MB or so.

Reports



Field	Description
Active	Tick the box to activate anti-spam reports.
Schedule	Click this button to define a schedule for sending quarantine reports. A simple dialog is opened

	allowing you to pick a schedule.
Run Now	Click this button to run spam reports immediately.
Enable quarantine reports	Check this box to have quarantine report emails sent to your users.
Enable spam folder reports	Check this box to have spam folder reports sent to your users.
Sender	Enter the sender you wish the reports to be sent from. This should be something meaningful – i.e. some valid email address.
From	Enter the ***From*** header information you wish to appear in the reports.
Report Mode	Choose one of the following: **New items** – the reports will only contain items that have been added since the last report. **All items** – the reports will always contain all items. *NOTE: Since version 12.1 it is possible to force mode (quarantine, spam) in GET parametr when launching manually via URL. Report can be forced to show only spam or quarantine by GET parametr "report_type" set to value "spam" or "quarantine".* ***Example:*** *Send only spam report:* *http://localhost:32000/reports/challengelist.html?report_type=spam* *Send only quarantine report:* *http://localhost:32000/reports/challengelist.html?report_type=quarantine* *Send both together:* *http://localhost:32000/reports/challengelist.html*
Log level	Select a level of anti-spam logs: ▪ **None** – no logs at all. ▪ **Summary** – only spam messages are logged. ▪ **Debug** – all messages and actions are logged. ▪ **Extended** – same as **Debug** for this service. *NOTE: It is strongly recommended to have the level set to **Summary** and select the **Debug** level only if you need to debug. After this debug, the level is to be set back to **Summary** (or **None**). If you choose debug reports, someone can call it remotely and see all addresses. For detailed information, refer to the warning (with an exclamation mark icon) at the end of this chapter.*
URL	Enter the URL of the confirmation page on the IceWarp Server. You should specify the port that IceWarp Server uses if it is not the standard (port 80). If you have a multi-domain server, you should use the system variable ***%%Recipient_Domain%%*** like so **http://%%Recipient_Domain%%:32000/reports/** The above setting says to use the domain of the email recipient, on port 32000, so for an email to john@icewarpdemo.com it will read **http://icewarpdemo.com:32000/reports** *NOTE: The IceWarp Server Web service must be running for this function to work.*
DB Settings	Click the button to open the **Database** dialog. Here, you can set a database for anti-spam reports. For more details, refer to the **F1 help – Shared Topics – Database Settings** chapter.

NOTE: Anti-Spam reports are launched via Web service.

*NOTE: For Anti-Spam report explanation, refer to the **Status Node – Logs – Example – Anti-Spam Reports** chapter.*

There are three variables related to spam reports:

- ***SpamLang*** – specifies the language of spam reports
- ***SpamReportsDateFormat*** – specifies the date format that spam reports will use
- ***SpamReportsTimeFormat*** – specifies the time format that spam reports will use

They can be edited by API Console.

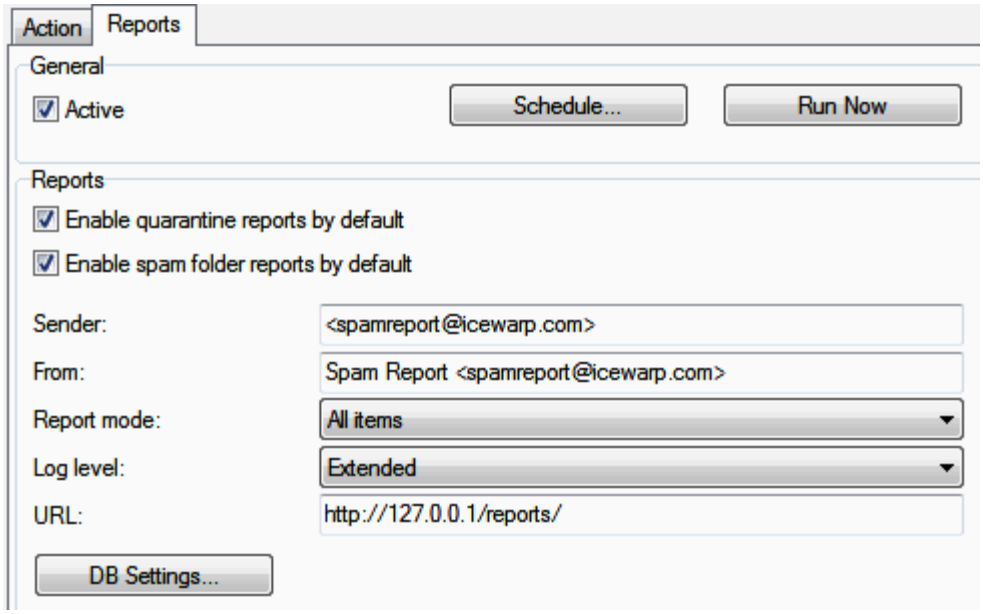
The appropriate formats are explained at ***http://cz2.php.net/manual/en/function.date.php***.

How to Set Anti-Spam Reports

1. **Enabling reports**

   Navigate to the **Anti-Spam – Action node – Action tab – Spam section** and set the ***Default spam folder mode*** field to ***Use spam folder***.

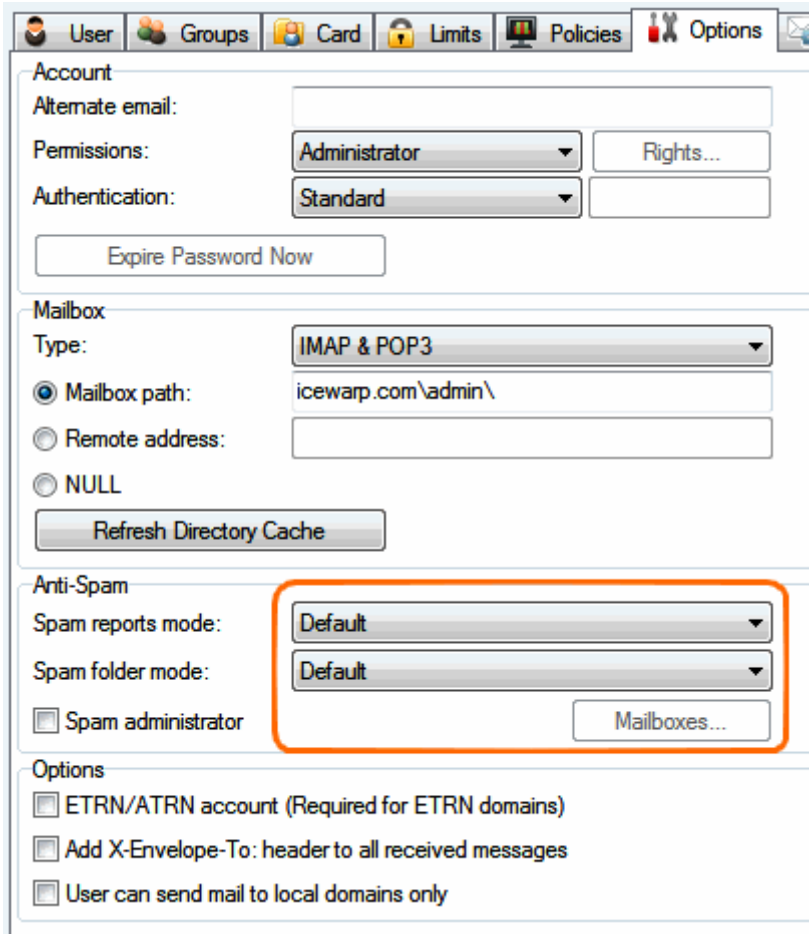
   Navigate to the **Anti-Spam – Action node – Reports** tab, enable reports (tick the boxes), set the ***Schedule, Sender, From header, Report mode*** and ***URL***.



2. **Specifying users/domains that will use reports**

   Now, reports are enabled for all users on your server, if you want to use reports only for certain users or domains, you need to change settings on the user level.

   Navigate to the **Management – <domain> – <user> – Options tab – Anti-Spam** section and set ***Spam reports mode*** and ***Spam folder mode***. (For more information, refer to the F1 help for this tab.)



3. **Using tool.exe**

   However you can use GUI to change settings, it is not convenient to set it for all domains/users manually.

   Therefore you can set these settings using this tool. Start the built in File Manager (click its icon within the GUI tool bar or press CTRL+SHIFT+F) and use the command line to run commands.

   tool set account *@* U_QuarantineReports x

   ****@* – all accounts on the server***

   ****@domain.com – all accounts at "domain.com"***

   user@domain.com – "user@domain.com" only

   Where ***x*** means:

   0 – Disabled

   1 – Default

   2 – New Items only

   3 – All items

Examples:

- You want to use reports, but you want to exclude some domain(s).

  If you follow step #1, all users will receive reports. You may want to exclude some domain/s:

  tool set account *@<domain> U_QuarantineReports 0

  Replace ***<domain>*** with the appropriate domain name.

  Other option is to create the ***bypass.dat*** file in the **spam/reports/** folder. This file should contain a list of domains that will be bypassed during processing of reports. This is very important for backup domains as these do not have users. It is recommended to use bypass only for backup domain. Use a single row for each domain name.

- You want to use reports only for one domain.

  The easiest way how to achieve it is to disable reports for all and then enable reports for the domain you want.

tool set account *@* U_QuarantineReports 0

This will disable reports for all users (this may take a while depending on a number of users on your server).

Now enable reports for domain/users you want:

tool set account *@<domain> U_QuarantineReports 1

NOTE: Default means settings on the Anti-Spam – Action node – Reports tab.

- You want to use different report type per some domain(s).

  You may want to use the ***All items*** mode for some domains and the ***New items*** one for others. Steps depend on the number of domains using one these modes. Should 80% of domains use ***All items***, the easier way is to set ***All items*** as the default mode (see step #1) and change the mode for the rest of domains.

  tool set account *@<domain> U_QuarantineReports 2

*NOTE: For backup domains, only quarantine reports are sent. If you want to have even spam reports sent, set spam message score (**AntiSpam – Action – Action tab – Score required to classify message as spam**) equal or lover than **Score required to quarantine message** (the same tab).*

Users that have accounts only within backup domains can access their quarantine queues without necessity to wait for reports. They have to:

** Insert the following address into a browser address field:*
<icewarp_server_hostname>/admin/index.html?view=gateway_login

** Fill in the **Email Address** and **Captcha** fields.*

** Follow the shown link to their current quarantines. The link is sent by email to the appropriate mail box.*

Different Report Schedules

You may want to set a different report schedule for some users or domains. To set it, do the following:

1. Create the **bypass.dat** file and insert it into the **<InstallDirectory>/spam/reports** folder.
2. Into this file, insert users and/or domains you want to bypass – one per line.

   Syntax for users is: ***<user's_email_address>***

   Syntax for domains is:***<domain>***

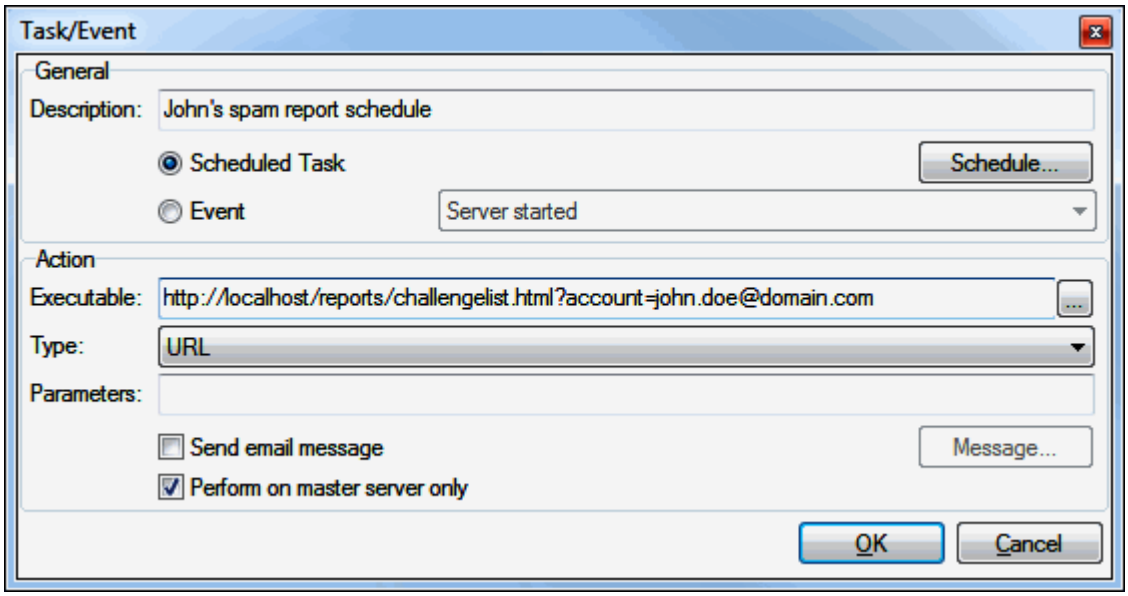
   Example:

   john.doe@domain.com

   alison.w@domain.com

   domain2.com

   This will exclude these users/domain(s) from a general spam report schedule.
3. Create a new task (**System – Tools – Tasks/Events**).



Click the ***Schedule*** button and set the wished individual schedule.

In the ***Type*** field, select the ***URL*** option. Enter the appropriate URL into the ***Executable*** field.

Syntax is:

for users: ***http://localhost/reports/challengelist.html?account=<user's_email_address>***

example: ***http://localhost/reports/challengelist.html?account=john.doe@domain.com***

for domains: ***http://localhost/reports/challengelist.html?domain=<domain>***

example: ***http://localhost/reports/challengelist.html?domain=domain2.com***

Do not forget to tick the ***Perform on the master server only*** box.

BEWARE: Reports URL can be executed by anyone, even remote users (and your user's emails could be seen). To prevent this, either change both ***SpamReports**** variables back to ***0*** (immediately after troubleshooting is done) or protect reports so they can be executed only within your server.

You may restrict access to the report script file on Web server (the **Web Site** dialog – **Access** tab) to localhost only:

URI = /reports/challengelist.html*

IP = NOT 127.0.0.1

ACCESS = DENY

NOTE ALSO: Debug logging consumes an unnecessary amount of resources.

NOTE: To obtain report details using this executable, use API console to set the following variables to the appropriate values: SpamReportsDebugLevel=1, SpamReportsLogLevel=4.

*NOTE: The timeout for spam reports is 32 minutes (1920 seconds), usually more then enough. If you notice timeouts in **phperror.log** (**<install_dir>/logs**) while debugging spam reports, you can increase **max_execution_time** in **php.ini** (**install_dir>/php**) and also **php.user.ini** – if used – so that such setting is preserved on upgrades.*

NOTE: If you execute custom reports in a task using your external host/IP, such as

http://externalip/reports/challengelist.html?account=xxx

Then your external IP needs to be in the rules listing of IPs that are NOT denied.

*Example: **127.0.0.1;externalIP***

*If you run customer reports using **http://127.0.0.1/reports/challengelist.html?account=xxx**, then*

*keeping **127.0.0.1** only in that field is enough.*

Details: http://forum.icewarp.com/forum/showthread.php?2702-Task-and-events-Issue

Quarantine

The Quarantine function of IceWarp Server allows you to place incoming messages in a pending queue awaiting authorization.

Users can manage their own pending queue via IceWarp WebClient.

Domain administrators can manage all pending messages in their domain via IceWarp WebClient or WebAdmin. Furthermore users can access their quarantine queues, whitelists and blacklists via WebAdmin.

Valid options for a pending message are:

- **Authorize** – which delivers the message and adds the sender to the quarantine whitelist and no further messages from him will be quarantined.
- **Deliver** – which delivers the message to the recipient without adding the sender to the whitelist.
- **Blacklist** – which simply deletes the message from the pending queue.

You can set whether external recipients of messages sent by your users are automatically added to the whitelist (see **Action**).

You can set a period of time after which pending messages are deleted from the queue (see later in this section).

You can also activate a Challenge Response system, whereby an un-authorized sender can prove he is a real person by visiting a website (see later in this section).

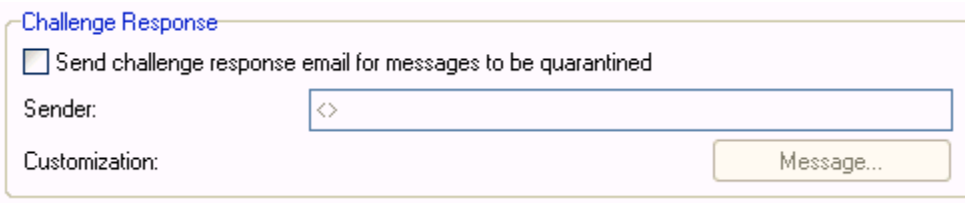
You can see the status of the pending queue and the quarantine whitelist in the **Spam Queues** node of the administration console or WebAdmin.

Field	Description
Active	Check this option to enable quarantine processing.
Quarantine	Click this button to jump to the quarantine queue in the **Spam Queues** node.

*NOTE: Access mode to the service can be set on both domain and user levels. See the appropriate places (**[domain] – Policies, [user] – Policies**).*

Field	Description
Remove Pending messages after Days	Specify the number of days a message is held awaiting action.
Deliver expired messages to mailbox	Check this box to have messages delivered to your users (marked as ***Spam***) when the quarantine period has expired.

as Spam	



The Challenge Response that is delivered to the sender by IceWarp Server contains a URL that must be accessed in order to process the sender's confirmation (see the **How it works** section).

This same engine is used by the Web-based administration and by WebClient.

Field	**Description**
Send Challenge response email for messages to be quarantined	Check this option to have a Challenge Response email sent to senders of quarantined messages. *NOTE: For this feature to work correctly you **must** set the Anti-Spam Reports URL correctly in the **System – Services – SmartDiscover – URL** section.*
Sender	Specify here the sender that will be used in the SMTP protocol. We do not recommend changing this from the default (empty) option, as this will cut down unwanted auto-responses etc.
Customization	Click the ***Message*** button to customize the Challenge Response message content. The **Message** dialog will open allowing you to specify the ***From:*** and ***Subject:*** headers, and the message body content. You can use system variables within the message body. *NOTE: The special variable %s **must** be included within the message body as this contains the URL to be visited.*

Example:

The following confirmation request message has been generated by the mail server in response to the sender user@icewarpdemo.com who sent a message to the user xxx@webmail.domaina.com.

The Anti-Spam Reports URL was defined as: **http://%%Recipient_Domain%%:32000/challenge/**

From:

To: <user@icewarpdemo.com>

Received: from webmail.domaina.com

by mail.icewarpdemo.com (IceWarp Server 10.1.2) with SMTP id DEMO

for <user@icewarpdemo.com>; Sun, 07 Mar 2004 01:48:16 +0100

Date: Sun, 07 Mar 2004 01:48:16 +0100

From: Challenge Response <info@icewarpdemo.com>

To: xxx@webmail.domaina.com

Message-Id: <812060168@mail.icewarpdemo.com>

Subject: [Challenge Response] Confirm your email by visiting this URL

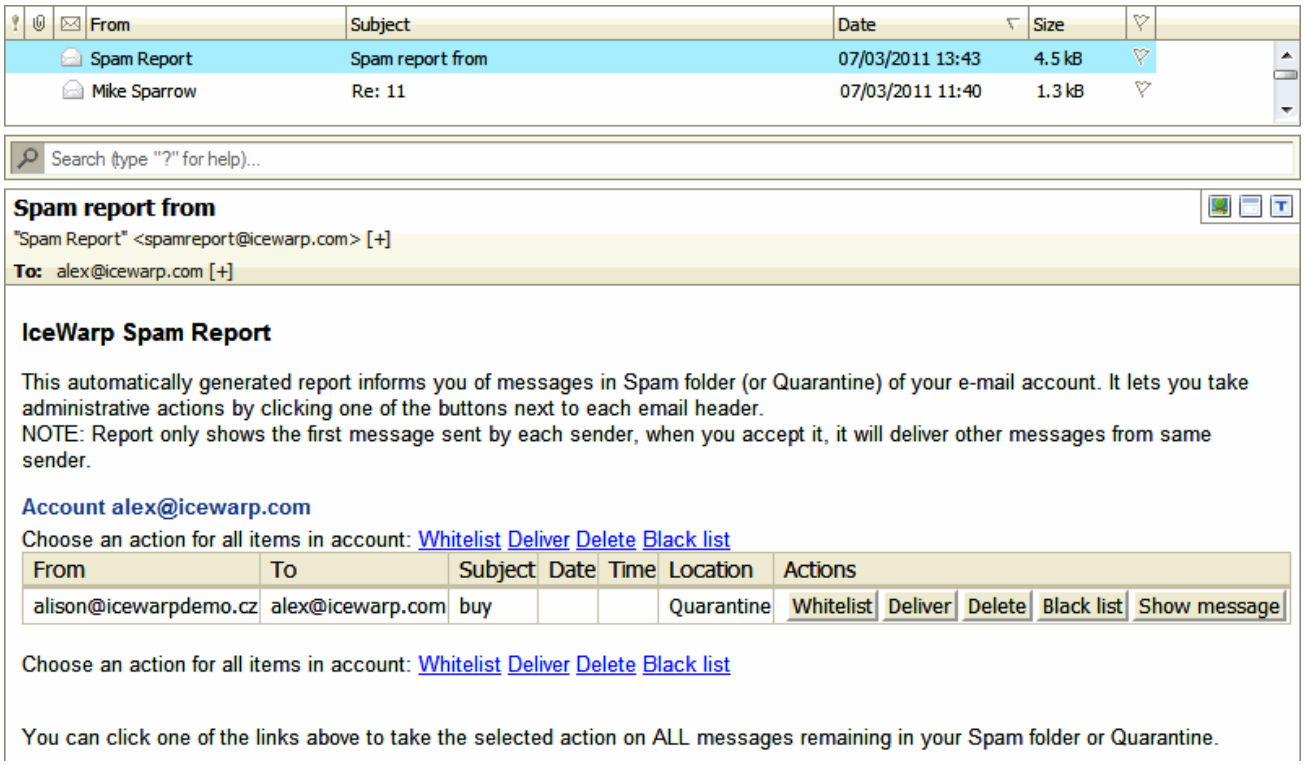
http://mail.icewarpdemo.com:32000/challenge/?folder=c42c1a770e2d6d07ff358b2c22d7cf71

To prove your message was sent by a human and not a computer, visit the URL below and type in the alphanumeric text you will see in the image. You will only be asked to do this once for this email address.

http://webmail.domaina.com:32000/challenge/?folder=c42c1a770e2d6d07ff358b2c22d7cf71

Quarantine Report

If enabled, as described above, each quarantine user will receive an email spam report listing quarantined messages with clickable links to deal with all listed messages and buttons for each single one:



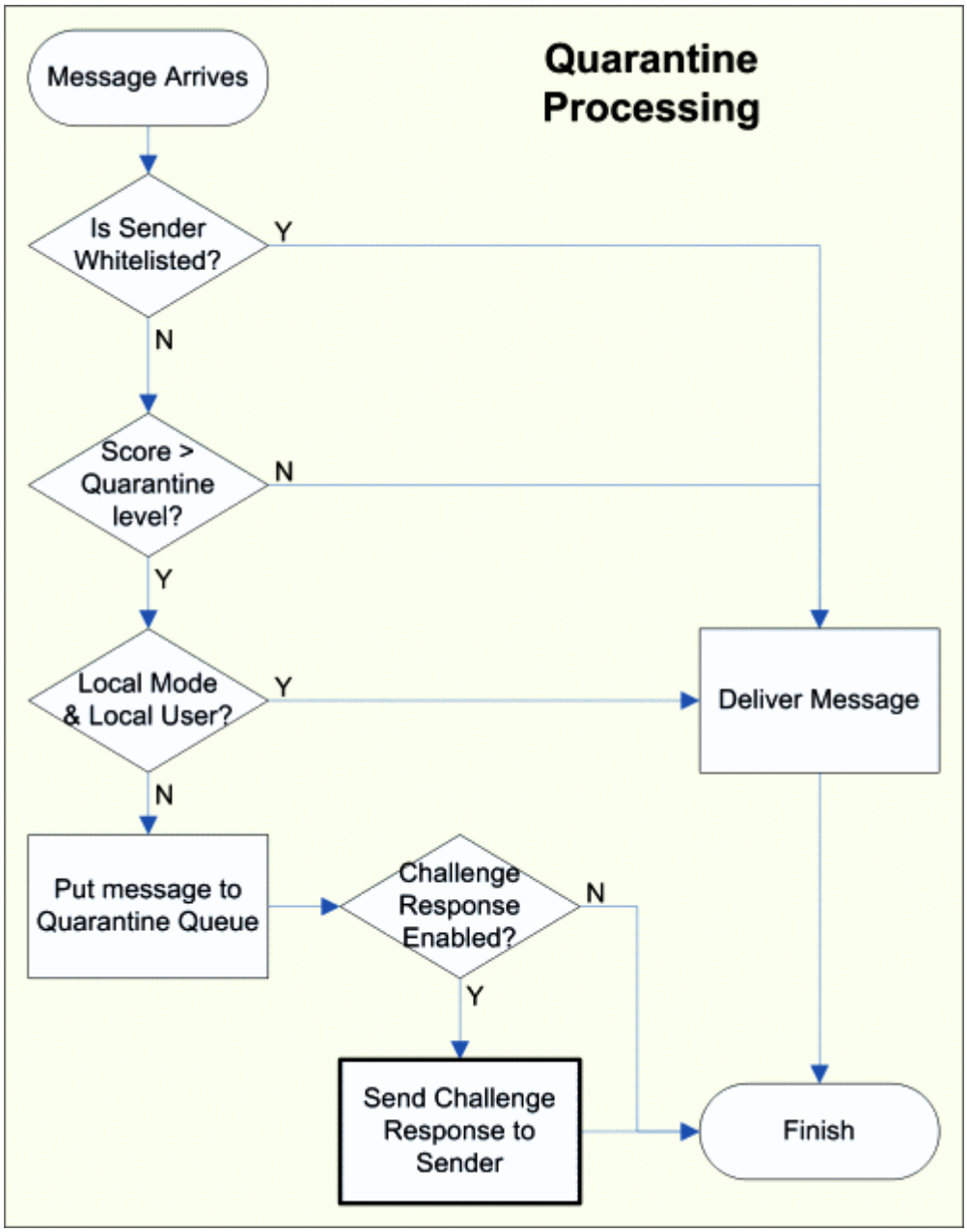
Details of the message are shown as in the screenshot above.

Button	Action
Whitelist	Delivers the message and whitelists the sender.
Deliver	Delivers the message to the recipient.
Delete	Deletes the message.
Black list	Adds the sender to the blacklist.
Show message	Opens a new browser window showing the message (including headers) in text format.

Processing for Incoming Messages

If the ***Quarantine*** function is enabled, all inbound message senders are checked against the quarantine whitelist. If the sender is whitelisted, the message is processed as normal. If the sender is not on the whitelist, the message is held in the quarantine pending queue.

In addition, if the Challenge Response system is enabled, a Challenge Response email is sent to the sender, which allows them to authorize themselves by visiting a web-page and effectively confirming he/she is a real person.

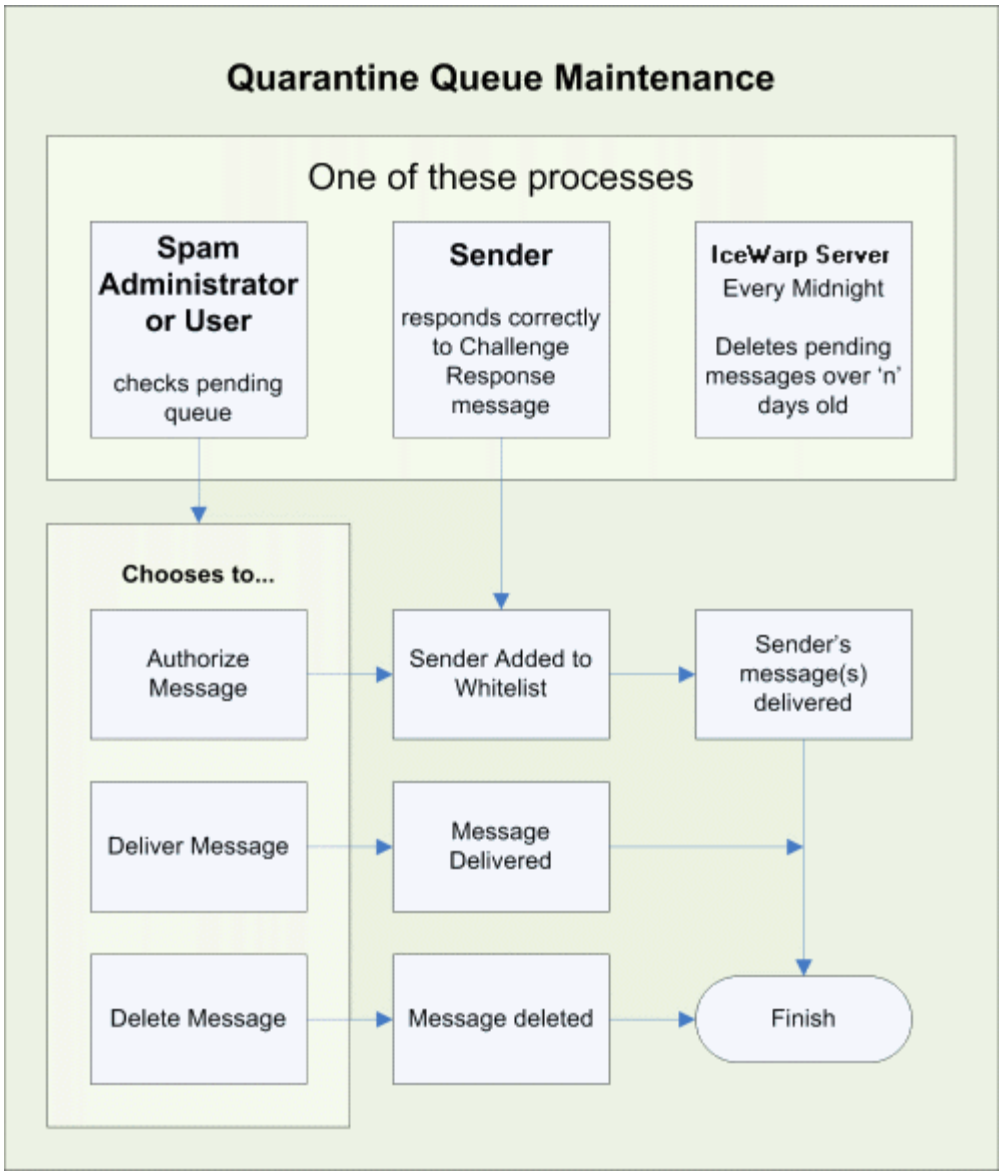


Processing for Pending Queue

Messages held in the pending queue are processed in multiple ways:

- Sender responds correctly to a Challenge Response email, and authorizes himself/herself.
- User checks his/her quarantine queue via IceWarp WebClient and chooses to ***Authorize, Deliver*** or ***Delete*** message(s).
- Spam administrator checks any quarantine queues he/she is responsible for via IceWarp WebClient or the administration console and chooses to ***Authorize, Deliver*** or **Delete** message(s).
- IceWarp Server automatically deletes a message after a selected number of days.

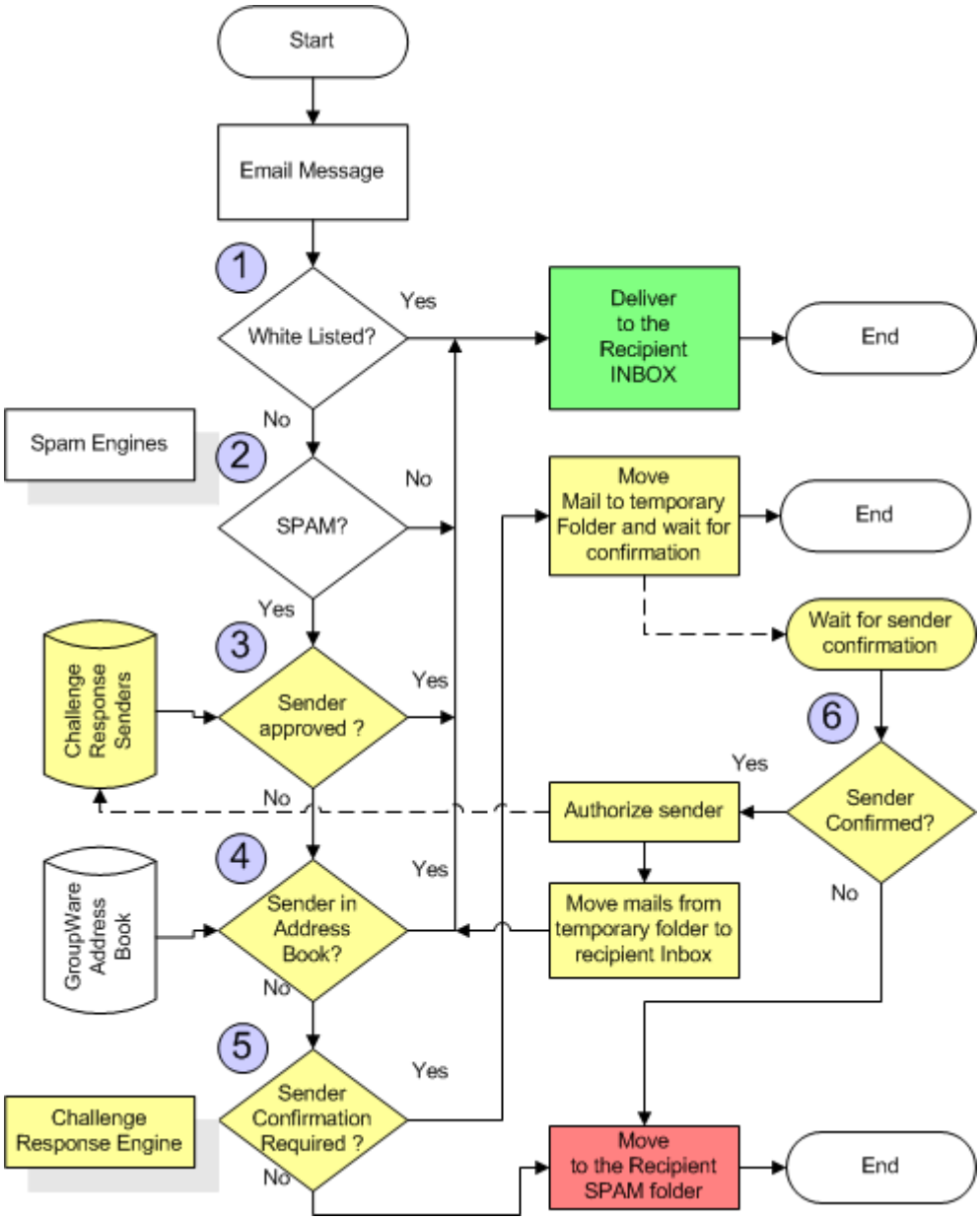
The following flowchart outlines the processing:



Challenge Response – How It Works

Challenge/Response is a system that requires the sender of an email to verify that he/she has actually sent the email. This confirmation must be provided manually by visiting a web page and entering a code.

The Challenge/Response system is a critical component of the full IceWarp Anti-Spam solution. The **yellow components** below are the full IceWarp Anti-Spam data diagram.



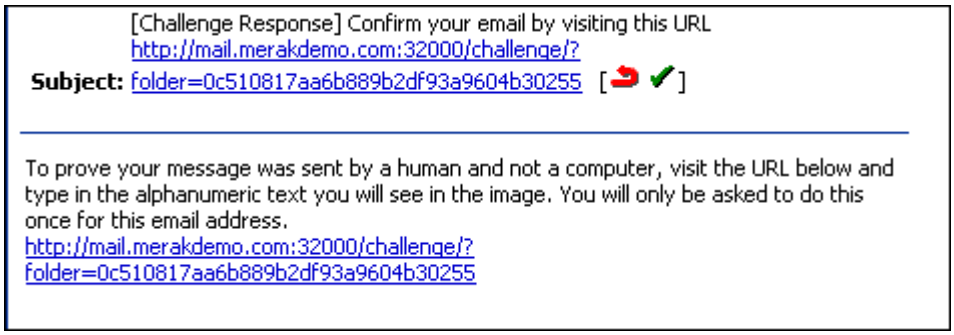
In the most typical situation, messages arrive at the Challenge/Response system after they have already passed all "whitelisting" possibilities as described in the Black & White listing techniques and are already marked as a spam.

- When an email is received by the server, it is not delivered to the recipient, but stored in a temporary folder. If more messages are sent from the same sender then all messages are stored in the same folder. Such messages are marked as "pending message(s)". If the pending message is not authorized within the specified number of days – it is automatically deleted.
- The IceWarp Server will generate the request for confirmation, which will be delivered to the email sender. It uses the sender from the SMTP protocol, which can be different from the ***Mail From:*** displayed in the message.
- The sender (if they exist) will receive the request for confirmation and must confirm it. The confirmation requires visiting a special web site and entering some characters into a text field. It prevents usage of automated confirmation systems.
- The IceWarp Server will receive the confirmation from the sender and will deliver the email(s) to the recipient. The sender is also entered into the "approved senders list" so confirmation will not be requested the next time.

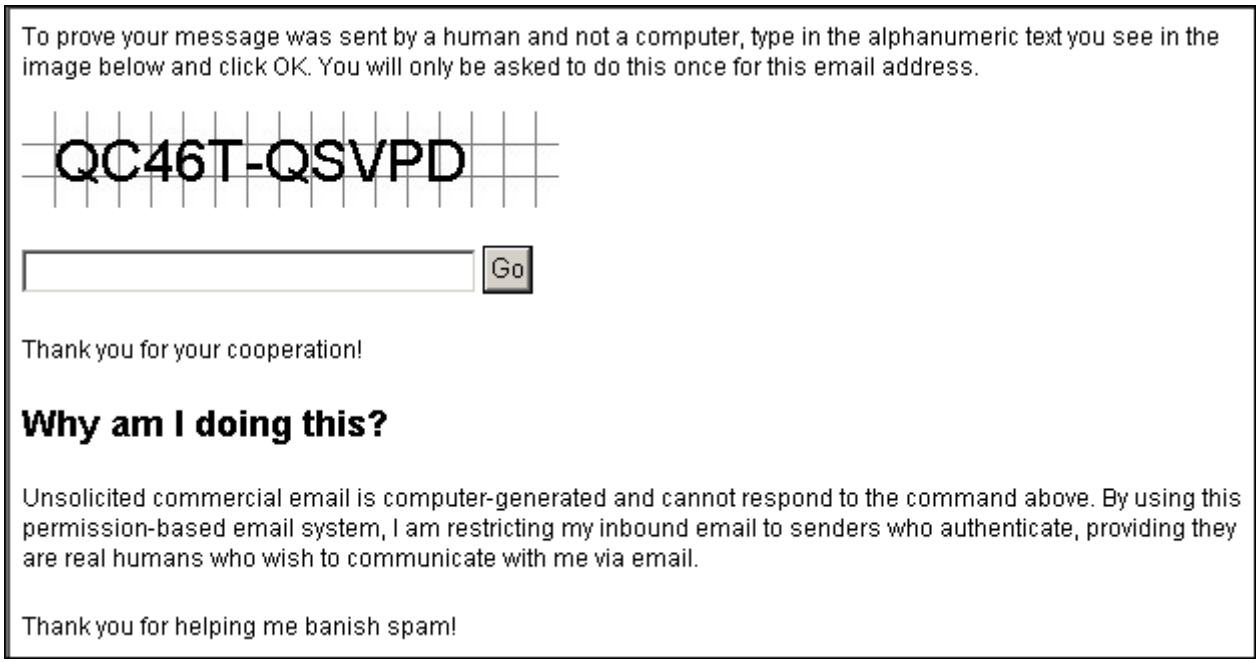
NOTE: *Emails with blank* ***Mail From*** *(it looks like* ***MAIL FROM: <>*** *in SMTP session) are bypassed by the Challenge Response engine. To handle such messages you should use* ***Content Filters*** *or* ***Black & White Lists****.*

Screenshot Examples

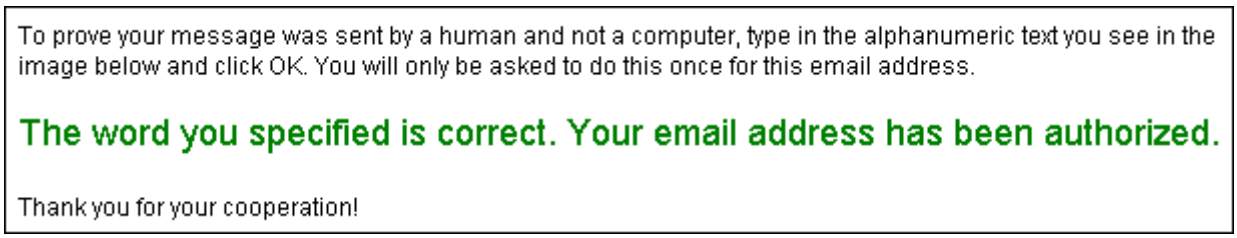
Request for Confirmation Sent by Mail Server to Sender



URL of the Page with Sender Confirmation Request



If Sender Enters the Code Properly they Are Automatically Authorized



Depending on the setup of the Challenge Response system, the sender can be authorized for just one recipient, or for all recipients on the server.

For information on "robotic" messages, refer to the **Domains and Accounts – Management – User Accounts – User – Mail** section.

SpamAssassin

SpamAssassin is an open source project dedicated to fighting spam. This software uses a set of complex rules to ascertain whether a message is spam or genuine. Basically, these rules check against typical spam templates.

These rules are constantly updated as new spamming techniques are introduced.

SpamAssassin is very good at identifying "phishing" messages that are trying to fool a user into giving out financial information.

SpamAssassin uses wide variety of local and network tests to identify spam signs. This makes it harder for spammers to identify one aspect which they can craft their messages to work around.

IceWarp Server uses the SpamAssassin rules but has its own in-house written engine to process them.

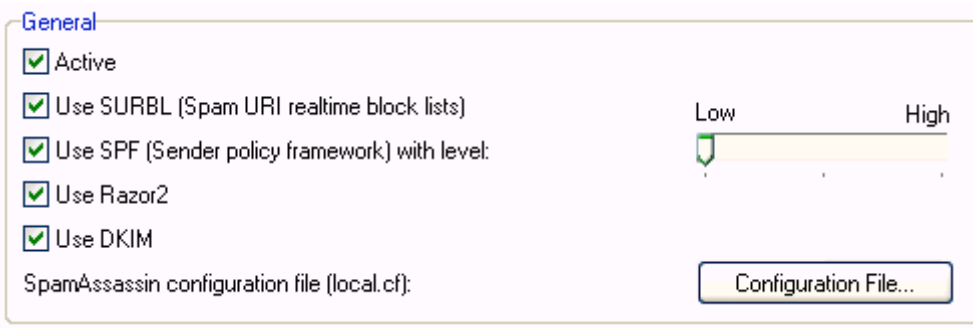
*TIP: Until the **whitelist_from_rcvd** variable is implemented, you can use the following workaround to whitelist a sender safely:*

Create a content filter that checks the sender (MAIL FROM) and compares with its true rDNS. Example for emails sent from Facebook:

Where Sender matches facebookmail.com

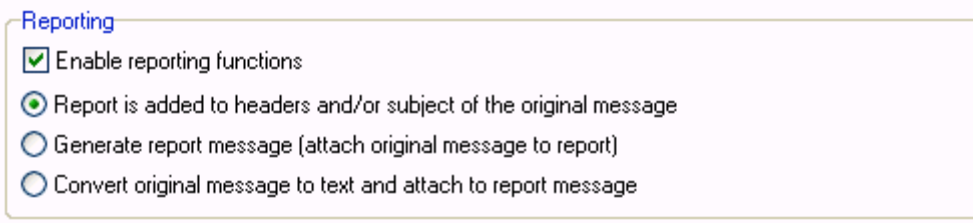
AND Where rDNS (PTR) matches facebook.com

Accept message



Field	Description
Active	Enables the SpamAssassin filters. *This option is recommended.*
Use SURBL	Check this option to enable Spam URI Realtime Blocklist technology. Rather than trying to identify spam senders, SURBL works by identifying the presence of the URI's of spam hosters in the message body. It is much more difficult for a spammer to change his host URI than anything else so this is a very reliable way of identifying them. SURBL is an excellent way of identifying "phishing" sources, i.e. sources that are well known for sending out messages intended to defraud people by the capture of bank login or credit card details. You can find more information at ***http://www.surbl.org/.*** *NOTE: This feature has to be enabled, if you want to run URIBL.*
Use SPF	Check this option to enable SPF (Sender Policy Framework) technology. SPF technology uses DNS to determine whether a message reported as coming from one domain and originating from another is valid. This relies on the DNS records being published, which is not always the case, and a "softfail" can occur, whereby the technology believes the sending host is not valid but cannot be sure. Use the slider to tell IceWarp Server what to do when the SPF check returns a "softfail". ***Low*** – adds 0.1 to the spam score ***Medium*** – adds 2.0 to the spam score ***High*** – adds 5.0 to the spam score - very strict! For an introduction to SPF please visit ***http://www.openspf.org/***.
Use Razor2	Check this option to have IceWarp Server use the Razor2 antispam technology. Razor2 is a distributed, collaborative, spam detection and filtering network. Through user contribution, Razor2 establishes a distributed and constantly updating catalogue of spam in propagation that is consulted by email clients to filter out known spam.

	Emails are identified by a hashed random portion of the email itself. Because the portion is random, and the position of the portion is constantly changing, it is very difficult for spammers to create a message that will bypass Razor2. You can find out more about Razor2 at ***http://razor.sourceforge.net/***. *NOTE: For Razor2 to function correctly, you will need to open the 2703 port on your firewall and/or router.*
Use DKIM	Check this option to enable DKIM technology. See ***http://antispam.yahoo.com/domainkeys/*** for a full introduction. If an incoming email from a domain which has a DNS DomainKey record is not signed, the total spam score is increased. If an incoming email is not signed at all, the score is also increased (but less than in the first case).
Configuration file	Click this button to open the SpamAssassin configuration file (**local.cf**). *Please, do not change any option within this file unless you are sure you know what you are doing. For information on creation rules within the **local.cf** file, refer here: **http://wiki.apache.org/spamassassin/WritingRules*** *Example of SpamAssassin tests for version 3.3.x: https://spamassassin.apache.org/tests_3_3_x.html* *NOTE: SMTP service restart is necessary after any SpamAssassin rule creation/change (within this file).* *To avoid that, you can update the spam update URL. In the **console – File – API console**, search for "spamupdateurl", double-click it and click OK, so it refreshes.* *Or use **tool.exe**:* ***tool modify system c_as_spamupdateurl http://www.icewarp.com/update/spam.xml*** *(For SpamAssassin rules (the **rule.cf** file), it is still necessary to restart the SMTP service.)* *NOTE: When creating customer rule files (**.cf** files), put them into the **/spam/rules/custom** folder, so that they do not get overwritten when IceWarp Server updates the **rules** folder.*

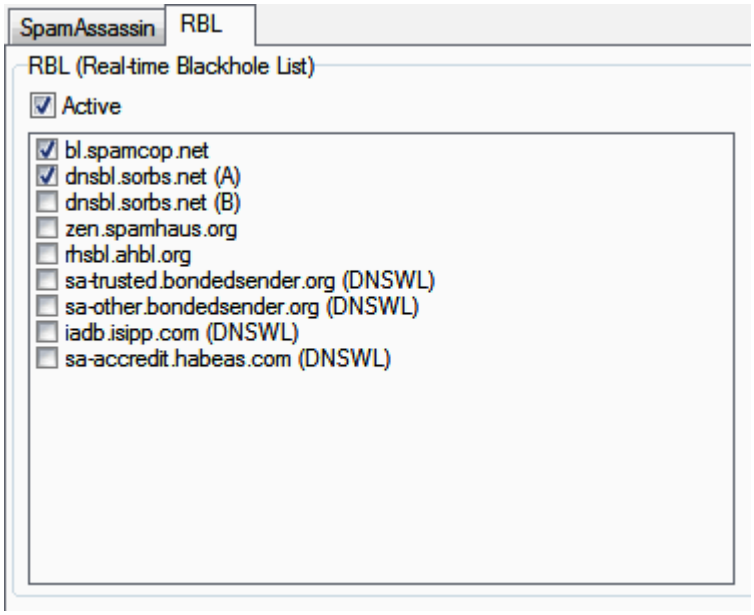


Field	Description
Enable reporting functions	Check this option if you wish to enable SpamAssassin reporting. Choose one of the three options for how you want reporting to function.
Report is added to headers and/or subject of the original message	The message will be received with modified headers. *This option is recommended.*
Generate report message (attach original message to report)	SpamAssassin report message will be received, with the original message attached.
Convert original message to text and attach to report message	SpamAssassin report message will be received, with the original message attached as a text file.

Field	Description
Log daily statistics to file	Enter a ***directory\file_name*** to have SpamAssassin statistics logged to a file. You can use the ***yyyymmdd*** style of a file name here to have the file dated.

SpamAssassin – RBL

RBL (Realtime Blackhole List) is a list of networks that are misused by spammers to send unsolicited emails. The idea behind RBL is simple: block traffic from spammer IP addresses and thus prevent the traffic from reaching a destination on internet.



Field	Description
Active	Enables the use of RBL servers.
RBL server list	Check the box against each RBL server you want to use. *NOTE: You should limit the number of servers you choose to query for RBL processing as this can have a detrimental effect on your server performance. Each server would have to be queried at least once for each incoming message, adding overhead to the processing.* *If a number of DNSBL hosts exceeds the limit of 4, a warning message is displayed.* RBL contains a list of IP addresses whose owners refuse to stop the proliferation of spam from their servers. The RBL usually lists ISPs whose customers are responsible for spam or email servers that are hijacked by spammers to send spam. *NOTE: Extended RBL codes are supported, see* ***http://www.us.sorbs.net/using.shtml*** *for further information.* *If you use* ***dnsbl.sorbs.net*** *as your RBL, it will return a code that signifies which blacklist(s) contained an entry.* *For example*

	127.0.0.3 is returned for an open SOCKS server *127.0.0.5 is returned for an open SMTP relay server* *NOTE: There are two **dnsbl.sorbs.net** items in the list (marked (A) and (B)). There are two different rules, both using **dnsbl.sorbs.net** – if you decide to use it, tick only one of them.*

SORBS – More Details

Notice that if you just enable SORBS here, SpamAsssasin default scores will be used. If you check the **spam/rules/***rbl.list* file, you will see SORBS is referred to as *RCVD_IN_SORBS_DUL;dnsbl.sorbs.net*.

Search now inside the **spam/rules/** folder for ***dnsbl.sorbs.net***.

You will find the *20_dnsbl.tests.cf* file with all the tests done on ***dnsbl.sorbs.net*** for each result code and you will find the *50_scores.cf* file where you can see what score is added according to each result code.

*NOTE: Refer to the **Mail Service – Reference – Rules – Content Filters** chapter for information on how to check DNSBLs and DNSWLs directly in content filters, disconsidering SpamAsssassin scores etc. and defining thus your own actions/score increase or decrease.*

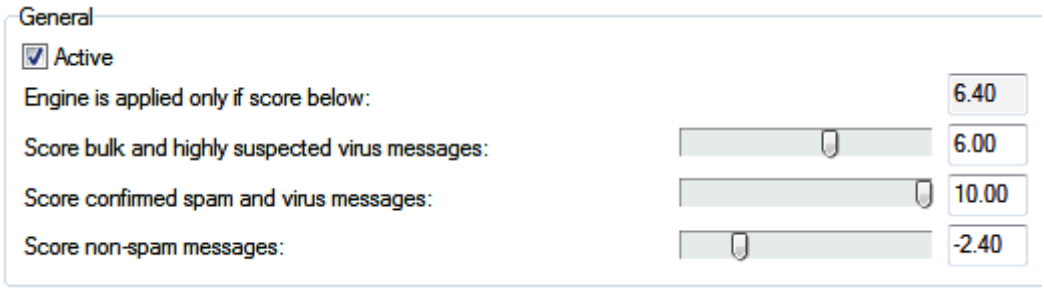
IceWarp Anti-Spam LIVE

IceWarp Server can use IceWarp Anti-Spam LIVE, an example of RPD (Recurring Pattern Detection) technology, as part of its fight against spam.

A Real-Time Detection Center analyzes large volumes of Internet traffic in real time, identifying new spam, virus and phishing outbreaks based on characteristic mass distribution patterns. Emerging outbreaks are usually identified moments after they are introduced onto the Internet.

This can significantly help in protecting your users from bulk and spam emails.

As with other IceWarp Anti-Spam technologies, IceWarp Anti-Spam LIVE is used to adjust the spam score of a message rather than to give a final judgment on the message:



Field	Description
Active	Enables Anti-Spam LIVE based on RPD (Recurrent Pattern Detection) technology. (This technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, protecting email infrastructures.)
Engine is applied only if score bellow	AS LIVE is run only on suspect messages to precise the scoring by SpamAssassin and other filters – either add or subtract some points. It is not run on messages that would be marked as spam anyway. This field indicates a spam score that is a limit for running IceWarp Anti-Spam LIVE. A message comes to IceWarp Anti-Spam LIVE with some spam score. In the ***Score non-spam messages,*** you set a score for messages that IceWarp Anti-Spam LIVE recognizes as OK. This score is subtracted from the score that a message has when coming to IceWarp Anti-Spam LIVE. If the result is higher than the spam score set in the **Anti/Spam – Action –*Score required to classify message as spam*** field, it is useless to apply IceWarp Anti-Spam LIVE because the message will

	still be a spam. Example: You have the ***Score required to classify ...*** value set to 4. The message comes to IceWarp Anti-Spam LIVE with the score of 7. The ***Score non-spam messages*** value is - 2.4. 7 - 2.4 = 4.6 This message will always have its score higher than 4 – it is useless to run IceWarp Anti-Spam LIVE. Another example: The message comes to IceWarp Anti-Spam LIVE with the score of 5. 5 - 2.4 = 2.6 IceWarp Anti-Spam LIVE is run.
Score bulk and suspected spam messages	Set the slider to an amount that will be added to the spam score if IceWarp Anti-Spam LIVE reports the message as bulk.
Score confirmed spam messages	Set the slider to an amount that will be added to the spam score if IceWarp Anti-Spam LIVE reports the message is a spam. Given the proven reliability of IceWarp Anti-Spam LIVE it is recommended that this be set at 9 or more.
Score non-spam messages	Set the slider to an amount that the spam score will be ***reduced*** by if IceWarp Anti-Spam LIVE reports the message as not a spam. The default value is ***0*** because reducing the score too much can result in False Positives – remember that LIVE is one of several technologies adding up to the overall score.
Suspected virus message action	
Confirmed virus message action	
Outgoing bulk and suspicious spam message action	
Outgoing confirmed spam message action	
Block Sender of outgoing virus message	
Notify administrator when account is blocked	Tick this box if you want to notify administrator when account is blocked

NOTE: The IceWarp Anti-Spam LIVE engine is only called for messages which are not classified as a spam by IceWarp Server's other AntiSpam engines, according to the ***Score required to classify a message as spam*** setting in **AS Action – General**.

IceWarp Anti-Spam LIVE Reasons – identified as LIVE:

Code Issued	**Reason**
Y	This message is flagged as highly likely spam by the IceWarp Anti-Spam LIVE servers.
H	This message is flagged as highly likely to be a bulk mail.
N	This message is considered genuine.

NOTE: Some servers block external access to port 80, thus they need to know what address is for AntiSpam LIVE to free it up in their firewalls. This information is in the **ctasd.conf** file

(**<InstallDirectory>/spam/commtouch**):

Server_address = Resolver%d.icew.ctmail.com

Where ***%d*** is some dynamic number.

IceWarp Anti-Spam LIVE Classifications

This table shows a cross-reference of the classification assigned by IceWarp Anti-Spam LIVE against the IceWarp Server reason code with a description of what each one means.

These IceWarp Anti-Spam LIVE classifications can be located within the antispam log.

Example line from antispam log:

*209.85.28.205 [1108] 05:19:44 PSC07843 '<cli10176@someone.com>' '<me@icewarpdemo.com>' 1 score 10.00 reason [SpamAssassin=1.60,Body=PE,**Live=H**,Sender] action SPAM*

and/or within the X_CTCH header of the message

Example X-CTCH header line

*X-CTCH: RefID="str=0001.0A090206.48EDBE9F.0245,ss=3,fgs=0"; **Spam="Bulk"; VOD="Unknown"***

*NOTE: If the message does **not** contain an X-CTCH header, then it has **not** been classified by IceWarp Anti-Spam LIVE and **should not** be reported!*

X-CTCH header	What it means	IceWarp Server Reason code	If mis-classified this is a...	Report this message to user...
Spam=Confirmed	Message is from a known spam source.	LIVE=Y	False Positive	aslive-genuine
Spam=Bulk	Message is not from a known spam source but has the characteristics of a bulk message.	LIVE=H	False Positive	aslive-genuine
Spam=Suspect See Note 1 below	Message is not from a known spam source but has a higher than normal distribution.	LIVE=N	False Negative	aslive-spam
Spam=Unknown	Message is not from a known spam source and has a normal distribution.	LIVE=N	False Negative	aslive-spam
Spam=Non-spam	Message comes from an IceWarp Anti-Spam LIVE trusted source.	LIVE=N	False Negative	aslive-spam
VOD=Virus	Message contains malware	LIVE=Y	False Positive	aslive-genuine
VOD=High	Message is highly likely to contain malware	LIVE=H	False Positive	aslive-genuine
VOD=Medium See Note 2 below	Message is suspected to contain malware	LIVE=N	See NOTE 2 below	See Note 2 below

VOD=Unknown See Note 2 below	Indeterminate threat level	LIVE=N	See NOTE 2 below	See Note 2 below
VOD=Non-virus See Note 2 below	Message confirmed as malware=free	LIVE=N	See NOTE 2 below	See Note 2 below

NOTE 1: Spam=Suspect is now deprecated and should not occur. If it does, then IceWarp Server classifies this as a legitimate message.

NOTE 2: IceWarp Anti-Spam LIVE does not replace the AV engine of IceWarp Server. For viruses, IceWarp Anti-Spam LIVE is only useful within the first few minutes of a new virus outbreak and as such IceWarp Server will only react to the highest probabilities that the message contains a virus. Therefore there is no point reporting false positives regarding virus detection by AS.

Reporting False Classifications

Report False Positives to **aslive-genuine@icewarp.<language code>** if the message is a genuine message, purchase confirmation, newsletter, etc. marked as spam/virus. This mailbox only accepts legitimate messages with classifications: Spam="Confirmed"/"Bulk" and VOD="Virus"/"High". Don't send messages with other classifications!

Report False Negatives to **aslive-spam@icewarp.<language code>** if the message is a spam, phishing, scam or hoax not marked as such. This mailbox accepts spam messages with classifications: Spam="Suspect"/"Unknown"/"Non-spam". Do not report viruses, malware or spam messages with other classifications!

The language code used should correspond to the language of the email. For example, if the email is in Czech, you should forward the message to aslive-genuine@icewarp.cz or aslive-spam@icewarp.cz.

If there is no corresponding country code, the message should be sent to support@icewarp.com, where our support team will attempt to assign it.

Your submission will be reviewed and dealt with as necessary.

DOs
Always review the messages you submit are all spam or all genuine – mixing these will negatively affect the service.
Messages are relayed to RDP Monitoring Team every 24 hrs – please only send current messages. Messages older than a week have probably already been reported and the service updated.
Create a ZIP archive of messages with the original headers including X-CTCH and saved in EML or MSG format or .imap/.tmp files copied from the server/mail repository. Prepare two separate archives for False Negatives and False Positives. Zip messages in the root of the zip file and do not password protect the zip. Name the zip either FP.zip for False Positives or FN.zip for False Negatives.
Messages should be saved in a raw format immediately upon receipt by the end user using the **Save As...** found in all popular email clients including IceWarp WebClient. Only EML and MSG formats retain original headers. The files can then be sent as attachments and eventually packed to ZIP. Messages saved in other formats will be skipped and not reported.

DO NOTs
If the original message has been forwarded/redirected anywhere between the end-user and you, it is useless to report it. It is essential to save them as EML or MSG immediately when received and then send these files as attachments, otherwise the original header information is lost and the mis-classification not reported.
Forwarding or redirecting a message to the address will be rejected. Sending an email with the message embedded (not packed in a ZIP) or using wrong password will be ignored.
Do not submit messages not including X-CTCH header. Do not submit regular IceWarp Anti-Spam false positives/negatives, messages without the X-CTCH header will be skipped and not reported anywhere.

Email Address to Report To

Submit the reports to the country/local partner corresponding to the message's ***language***, e.g. ***aslive-genuine@icewarp.fr*** if the message is in French.

The country partner will review the submissions (not mixed FPs and FNs) and forward them to IceWarp, who will in turn contact the RDP Service Monitoring Team and work with them on updating the service.

This step is required to ensure the credibility of the submissions.

If there is no country partner associated with your language, the messages should be sent in two files (FP.zip and FN.zip) attached to a support ticket or directly to ***support@icewarp.com***, and the support engineers will review the format is correct.

*NOTE: Messages to **support@icewarp.com** sent in languages other than English will be ignored if not agreed before.*

Bayesian

Bayesian filters are a statistical approach to spam identification. A database of words, and their frequency of occurrence in both spam and ham messages, is built up and used to give a probability that a word contained in a message identifies it as a spam.

Field	Description
Active	Enables the Bayesian filters. It is recommended that this option is enabled.
Compact the Bayesian Database	By clicking this button, you will remove words that occur at a low frequency. These words are mostly random words that you usually see included in a spam email. By compacting your database, the accuracy of the Bayesian filter will increase because these low frequency words have been removed. *Only the **User Reference Base** is compacted by this button.*

Field	Description
Auto learn	Check this option to enable IceWarp Server's Bayesian Auto Learn function. Messages with spam scores in the range you specify will automatically be indexed to the User Reference Base.
Index spam message if score higher than	Specify a value here by moving the slider. All messages assigned a score equal to or higher than this value will be indexed as spam messages.
Index genuine message if score lower than	Specify a value here by moving the slider. All messages assigned a spam score equal to or lower than this value will be indexed as genuine messages.
Index genuine message if trusted IP or authorized session	Check this option to have messages indexed as genuine if it comes from a trusted IP address or from an authorized session (i.e. outgoing sessions that are SMTP authorized, POP before SMTP authorized, or from a trusted IP)

Field	Description
Stop words	Contains the words that will be ignored during the Spam Reference Base update (indexing process). We highly recommend that you propagate this with words that are often used in your own internal communications, such as company name, products, services, etc. Separate them using semicolons.

Bayesian Filters – Basic Explanation

Bayesian filters, as implemented within IceWarp Server, use two reference databases to decide the probability that a message is a spam:

The **Reference Base**, which is built and supplied by us, uses real-world messages in a real-world mail server. Updates are supplied through the AntiSpam update function.

The **User Reference Base**, which is built by IceWarp Server using the Auto Learn and/or Learning Rules functions, and uses actual messages passing through the server, and consequently becomes much more specific to the individual installation.

User Reference Base information overrides Reference Base information.

Bayesian filters are based on the Bayesian probability theory. This theory says that the probability something will happen is the same as the probability that it has happened in the past. For them to work correctly a good selection of both spam and real (ham) messages should be analyzed.

Its implementation within IceWarp Server is as follows:

Take the probability that a spam message contains a certain word.

Multiply by the probability that any email is spam.

Divide by the probability that a ham message contains the certain word.

Gives you the probability that this message is spam.

Example

Assume:

We have received and analyzed 100,000 messages in total.

80,000 messages are spam.

*48,000 spam messages contain the word **viagra**.*

*400 ham messages contain the word **viagra**.*

Then:

*The probability that spam contains **viagra** = 48,000 / 80,000 = 0.6*

The probability that a message is spam = 80,000 / 100,000 = 0.8

*The probability that any message contains **viagra** is (48,000 + 400) / 100,000 = 0.484*

*So Bayesian theory says the probability that a message containing **viagra** is spam = 0.6 * 0.8 / 0.484 = 0.991*

*Meaning a message containing **viagra** has a 99.1% chance of being spam.*

We recommend an initial Auto Learn period of about two weeks, and a Compact and re-learn every 3-4 months at least. This will allow the User Reference Base to follow any changes in company message content (for example, the company start selling mortgages)

The User Reference Base can hold a maximum of 100,000 words. (This limit can be changed – use the *C_AS_SpamBayesMaxWords* API variable.) You can see how many words are actually stored in the **General** tab.

Once the limit is reached you should Compact the database (which removes lower frequency, less important, words) and enable the Auto Learn feature again for a time.

The Reference Base is contained within file **<install_dir>/spam/spam.db**

The User Reference Base is contained within file **<install_dir>/spam/spam.usr**

spam.db and spam.usr Files

These files include records of spam probability of given words:

reseller 38768 55 999999999999999999

return 38953 128 190

revealed 38891 0 16

where items on each line are:

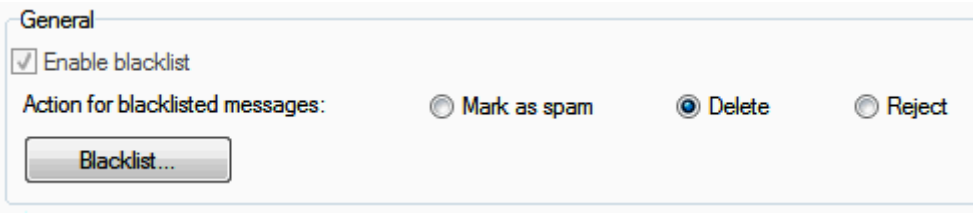
- word itself
- timestamp of the last modification (Delphi time, number of days from 1.1.1900)
- how much genuine messages contained this word
- how much spam messages contained this word

NOTES: Sometimes, the same number is subtracted from both spam and genuine counters to keep the numbers low. So, the third example record does not mean that there was not any spam message with this word.

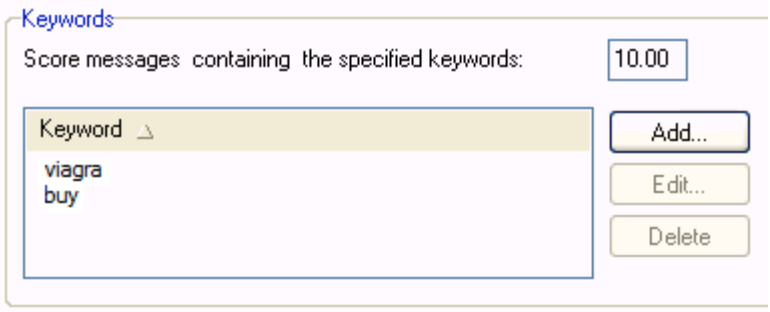
These numbers are only 32-bit ones, thus they cannot be higher than 4294967295. In the case this number is exceeded, the appropriate record can look a bit strange – see the first record.

Black & White Lists

Blacklist



Field	Description
Enable blacklist	Check this option to enable **Blacklist** processing to modify the spam score of a message. *NOTE: When you enable **Quarantine, Blacklist** and **Whitelist** are enabled at the same time. With **Quarantine** enabled, it is not possible to disable them.* *NOTE: For full automatic blacklisting, enabled Spam Folder is required.*
Action for blacklisted messages	Select the desired behaviour: ▪ **Mark as spam** – messages from blacklisted senders are treated as spam. ▪ **Delete** – messages from blacklisted senders are deleted immediately. ▪ **Reject** – messages from blacklisted senders are rejected.
Blacklist	Click this button to jump to the Spam Blacklist queue.



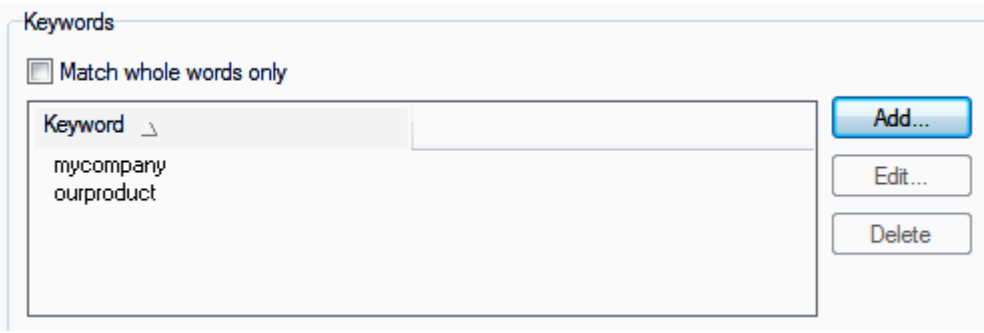
Field	Description
Score messages containing the specified keywords	Enter a value to modify the score by.
Keywords	This section allows you to define a list of words that, if found within a message, will cause the message to have its spam score increased. Size of this field is limited to 256 characters. If you need to use longer list of keywords, insert them into a ***.txt*** file and enter a fully qualified path to the file into this field. (It is possible to use more .txt files, i.e. to enter more than one path.) Items are evaluated in the order of appearance in the field.
Add	Click this button to add a word to the list.
Edit	Click this button to modify the selected word.
Delete	Click this button to remove a word from the list

For information on "robotic" messages, refer to the **Domains and Accounts – Management – User Accounts – User – Mail** section.

Whitelist

Field	Description
Enable whitelist	Check this button to enable anti-spam **Whitelist** processing. *NOTE: When you enable **Quarantine, Blacklist** and **Whitelist** are enabled at the same time. With **Quarantine** enabled, it is not possible to disable them.* *NOTE: For full automatic whitelisting, enabled Spam Folder is required.*
Whitelist	Click this button to switch to the **Spam Queues** node, with the **Whitelist** selected.

Field	Description
Whitelist trusted IPs and authenticated sessions	Check this option to add IP addresses in "trusted" lists to the whitelist automatically. Also adds authenticated session items to the whitelist. *NOTE: IP addresses are whitelisted but NOT added into the database*
Whitelist local domain senders	Check this option to have senders from local domains added to the whitelist. IceWarp Server checks both ***Sender*** and ***From*** headers – they must represent an existing local account. *NOTE: These senders are whitelisted but NOT added into the database.*
Whitelist senders in groupware address books	Check this option and IceWarp Server will add addresses from recipient's GroupWare address books to the whitelist automatically. *NOTE: These senders are whitelisted but NOT added into the database.*
Whitelist senders in instant messaging server rosters	Check this option and IceWarp Server will add addresses from recipient's IM rosters to the whitelist automatically. *NOTE: These senders are whitelisted but NOT added into the database.*
Auto whitelist trusted email recipients to database	Check this option to have all trusted recipient addresses added to the whitelist database. Database "level" depends on the ***Anti-Spam mode*** feature setting (see **Anti-Spam – General – Other**). E.g. when it is set to ***Domain*** a trusted address is added into the recipient's domain whitelist. *NOTE: When an IceWarp Server user sends an email, the recipient's email address is considered as a trusted one.*



Field	Description
Match whole words only	Tick the box if you want to have whitelisted only whole words. Otherwise all words containing defined keywords are whitelisted too. Example: Keyword: *egg*, the *Match...* box not ticked – also expressions *eggbeater*, *egghead*, *eggplant*, etc. will be whitelisted.
Keywords	This section allows you to define a list of words/phrases that, if found within a message body, will cause the message to be bypassed by Anti-Spam processing. Size of this field is limited to 256 characters. If you need to use longer list of keywords, insert them into a ***.txt*** file and enter a fully qualified path to the file into this field. (It is possible to use more .txt files, i.e. to enter more than one path.) Items are evaluated in the order of appearance in the field.
Add	Click this button to add a word/phrase to the list.
Edit	Click this button to modify the selected word.
Delete	Click this button to remove a word from the list

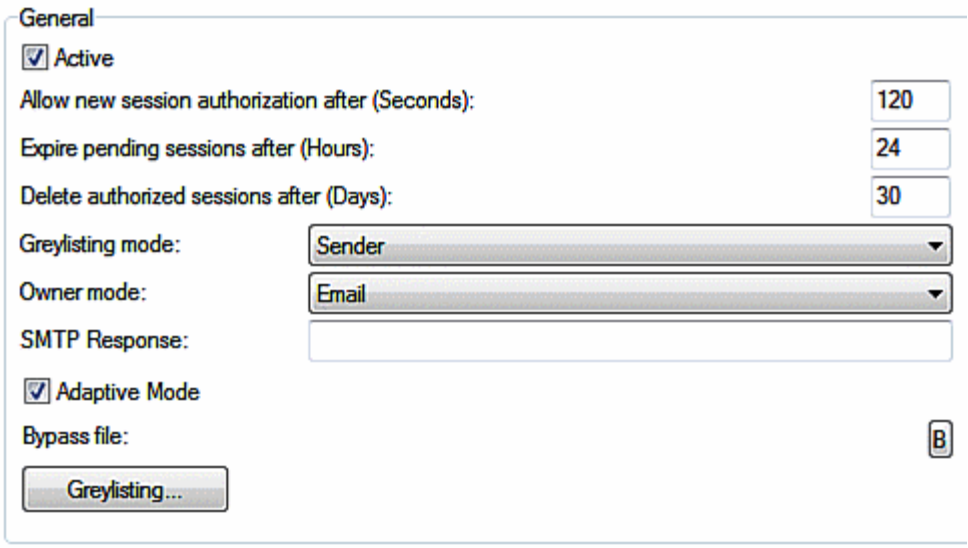
*NOTE: There is no special flag for auto-whitelisted items. However, one distinction can be the **SndIP** column (SQL Manager – antispam.db). Auto-whitelisted items have these fields filled with IP addresses, whitelist records added manually (either from WebClient or console) have these fields empty.*

*So, for example the **DELETE FROM Senders WHERE SndIP !=''AND SndWord ='';** command would delete all auto-whitelist entries. (Use with care, backup your DB.)*

Greylisting

Most spammer's servers will try to deliver a message to the receiving server and give up if they do not get a quick response. A "real" server will retry the session after a period of time.

Greylisting allows you to reject an incoming session for a specified period of time. This will deter many spam servers from sending their messages.



For Greylisting these local bypasses are important:

Bypass trusted IPs,

Exclude outgoing messages from spam scanning,

Local-local bypass filter,

Greylisting bypass file (greylist.dat)

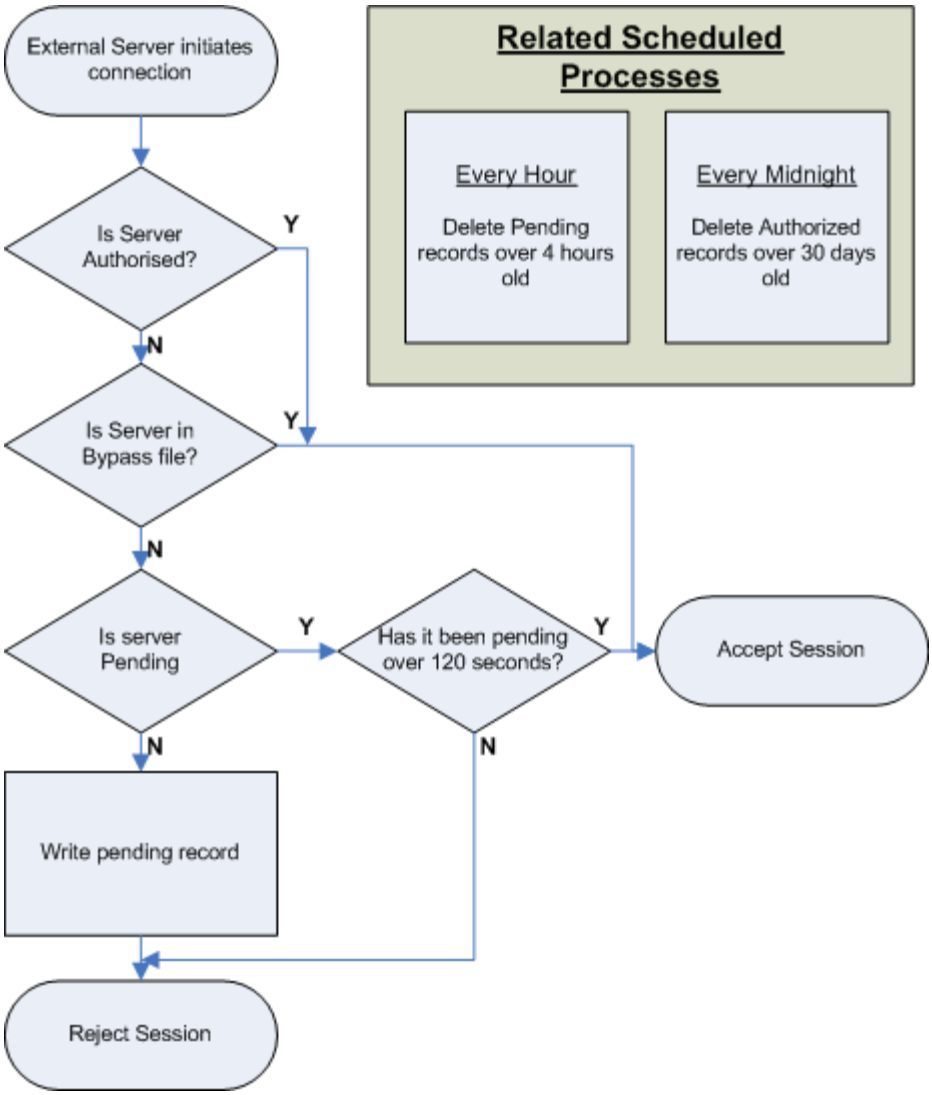
If these are not applied, the users will get a temporary error 4.5.1 in their mail clients and will be allowed to send the message after x seconds.

Field	Description
Active	Check this option to enable **Greylisting**.
Allow new authorization after (Seconds)	Specify the amount of time that incoming connections should be rejected. Any retries within this time period will be rejected.
Expire pending sessions after (Hours)	Specify the amount of time after which any "pending" IP addresses are expired within the database. *NOTE: "Pending" addresses are addresses which have tried to connect and have been rejected by greylisting.*
Delete authorized sessions after (Days)	Specify the number of days that an authorized IP address is held in the database. A value of 0 means authorized IP addresses will never be deleted. *NOTE: "Authorized" addresses are addresses that were rejected by greylisting, but then accepted at a later retry from the address.*

Greylisting mode	Select the data that should be stored in the **Greylisting** database. There are four possible modes: ▪ ***Sender*** – The email address of the person sending the email. ▪ ***IP*** – The IP address of the machine sending the email. ▪ ***Sender&IP*** – Both of the above. ▪ ***IP + HELO/EHLO –*** IP address of the machine sending the email and hostname sent in the HELO/EHLO command at the beginning of the SMTP session. *NOTE: The recommended mode is **Sender**.* *Multi-IP systems, such as gmail, may retry the connection from a different IP address, and this would in turn be greylisted.*
Owner mode	Choose from two options: ***Email*** Select this option to have a greylist associated to individual email accounts. Once a message comes out of greylisting it is only accepted for that specific account. ***Domain*** Select this option to have the greylist entry associated to the domain. So once a message passes greylisting it is accepted for the whole domain.
SMTP Response	If you wish, you can specify a custom SMTP response to be used when a connection is rejected by greylisting. If left blank, the default SMTP response message is returned.
Adaptive Mode	If enabled, it changes the way how greylisting is applied to senders. When a sender sends an e-mail, classified as a spam, greylisting is turned on for him/her. Hence, his/her next attempts are greylisted.
Bypass file (greylist.dat)	Click the B button to edit a greylisting Bypass file, where you can specify users, domains and IP address ranges that will not be greylisted. Examples are given within the file.
Greylisting	Click this button to jump to the Spam Greylist queue.

Greylisting Flowchart

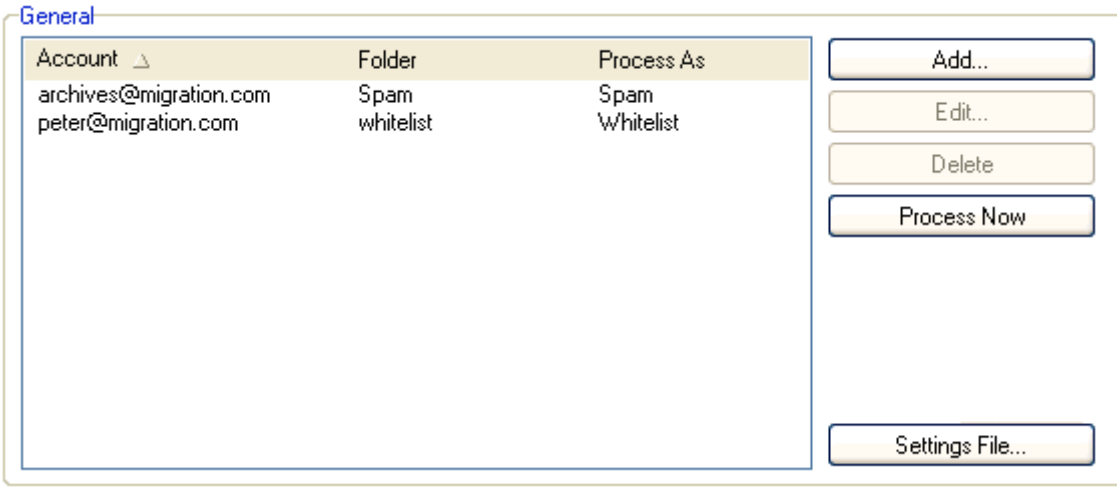
The following flowchart is designed to give you an idea of how greylisting works. It is not an accurate representation of the code, just a visual guide to the philosophy.



Learning Rules

With spammer's techniques evolving all the time there are occasions when a message will be incorrectly identified as genuine and, more rarely, incorrectly identified as spam.

The Learning Rules section allows you to let your users address these situations automatically, either by having an incorrectly identified message indexed, or by adding the sender of the message to the Blacklist or Whitelist.

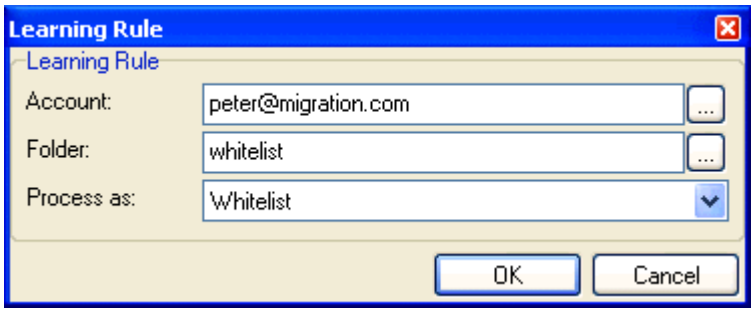


Queues can be either

- a mailbox folder identified by its account name
- any IMAP folder

Messages should be copied or moved to the relevant destination. We recommend that you copy genuine message and move spam messages as the messages within these locations are deleted after the indexing process completes.

Button	**Description**
Add	Click the button to create a new rule. The **Learning Rule** dialog opens.
Edit	Select a rule and click the button to edit this rule. The **Learning Rule** dialog opens.
Delete	Select a rule and click the button to delete this rule.
Process Now	Messages are processed at midnight. Click the button to process messages immediately.
Settings File	Click this button to open the settings file in a plain-text editor. You will see any rules you have created and can add more rules with the correct syntax. In the editor, click the ***Comment*** button to open an informational pane explaining the syntax.



Field	**Description**
Account	If this queue is to based on a mailbox folder enter the account here. The '...' button will open the standard **Select Item** dialog. WARNING: All messages in this mailbox will be deleted after the indexing is complete. We recommend you use separate mailbox folders for indexing purposes and either copy (for good messages) or move (for bad messages) relevant messages to the folder.
Folder	If this queue is to be based on an IMAP folder, enter the folder name here.

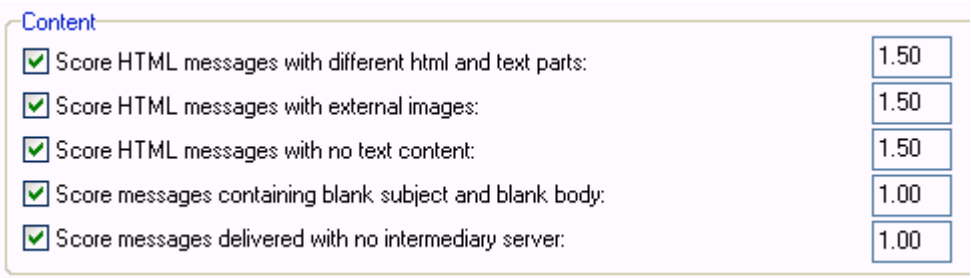
	The '...' button will open a standard dialog allowing you to navigate to the folder required. WARNING: All messages in this IMAP folder will be deleted after the indexing is complete. We recommend you use separate IMAP folders for indexing purposes and either copy (for good messages) or move (for bad messages) relevant messages to the folder.
Process as	Select how messages will be processed: ***Blacklist*** – This queue contains messages whose senders should be blacklisted. ***Whitelist*** – This queue contains messages whose senders should be whitelisted. ***Bayes – Add – Spam*** – Use this queue for messages which are spam but not marked as spam. The message content is indexed as spam. ***Bayes – Add – Genuine*** – Use this queue for messages which are genuine. The message content is indexed as genuine. ***Bayes – Change – Spam –> Genuine*** – This queue is used to re-index messages that have been incorrectly indexed as spam for some reason. The message content will be de-indexed as spam and indexed as genuine. ***Bayes – Change – Genuine –> Spam*** – This queue is used to re-index messages that have been incorrectly indexed as genuine for some reason. The message content will be de-indexed as genuine and indexed as spam. *NOTE: For blacklisting to work correctly, it must be enabled (See **AntiSpam – WhiteList** (see "Whitelist" on page)).* *It is also valid to have multiple queues for each type.*

It is recommended to use shared IMAP folders for these queues. This will allow your users to make them visible in Outlook and then they can copy any messages that need to indexed directly into them from their clients.

Miscellaneous

Content

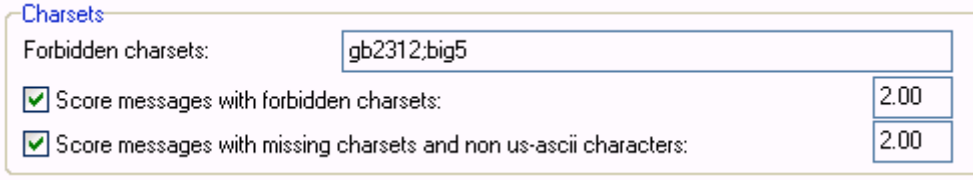
The Content Filter selection has been developed to catch the most common spam messages, which are usually incorrectly formatted, or "blasted" at your server to multiple recipients, or the content structure is simply not typical of a regular messages created by regular email clients.



Check an option and enter a value. The value will be added to the spam score if the test evaluates as true.

Fields	Description
Score HTML messages with different html and text parts	If a message contains HTML and plain-text parts, they should match exactly. Many spam emails have both parts, but they do not match. Check this option IceWarp Server to increase the spam score of such messages. *NOTE: Some email clients do not generate the plain-text part correctly, so this option should be used with care, especially if you are checking outgoing messages.*
Score HTML messages with external images	It is unusual for a normal message to contain a link to an external image. Check this option IceWarp Server to increase the spam score of such messages. *NOTE: SmartAttach use does not trigger off this feature.*
Score HTML messages with no text content	HTML messages should have a text part. Check this option IceWarp Server to increase the spam score of messages without text content.
Score messages containing blank subject and blank body	Messages should have at least a subject or some content. Check this option IceWarp Server to increase the spam score of messages without subject and body.
Score messages delivered with no intermediary server	Regular messages tend to be delivered via an intermediary server (e.g. their ISP's server or a corporate server). Check this option IceWarp Server to increase the spam score of messages without any intermediary server.

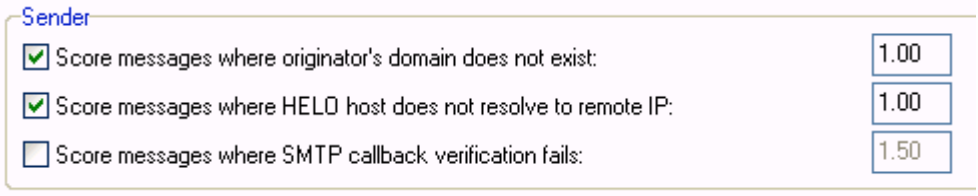
Charsets



Field	Description
Forbidden charsets	Specify a list of charsets that you consider likely to be a spam.
Score messages with forbidden charsets	Check this option to have IceWarp Server increase the spam score of messages containing any charsets listed. The spam score is increased by the value you specify.
Score messages with missing charsets and non us-ascii characters.	Check this option to have IceWarp Server increase the spam score of messages with missing charsets or containing non us-ascii characters.

BEWARE: If you send messages through IceWarp Server from a website HTML form, you should be aware that these messages will often contain high-value characters (for example, in some foreign names). Always try to construct the message with a correctly defined charset and consider whitelisting the IP address of the website.

Senders



Field	Description
Score messages where sender's domain does not exist	Check this option IceWarp Server to check whether the sender's domain exists. If it does not, IceWarp Server will increase the spam score by the value specified.
Score messages where HELO host does not resolve to remote IP	Check this option and IceWarp Server will check whether the hostname given in the HELO command resolves to the same IP address that the message is being delivered from. If it does not, IceWarp Server will increase the spam score by the value specified.
Score message where remote IP does not verify to a valid SMTP server	Check this option IceWarp Server to verify whether the IP address that is delivering the message is a valid SMTP server. If it does not, IceWarp Server will increase the spam score by the value specified. WARNING: This is achieved by attempting to connect to port 25 (the standard SMTP port) of the domain this message is coming from. A response to this could take up to 5 seconds and could therefore seriously slow down your server.

Spam Scores Concept

One of the first things you need to understand is the Spam Score concept.

AS IceWarp Server processes messages with its many Anti-Spam technologies and checks, it modifies a Spam Score value dependent on the results of each test.

The Spam Score is a value from 0.00 to 10.00 that indicates the probability that the message is a spam, with 10.00 being an indication that the message is very likely to be a spam.

Some of the settings within IceWarp Server allow you to set a value to modify the Spam Score (for example **Content Checks**). The value you enter in this section is the amount that IceWarp Server will modify the Spam Score by. So if you enter 1.5 for ***Score message containing blank subject and blank body***, the Spam Score will be increased by 1.5 if that test evaluates as true.

Rules Customization – local.cf File

The **local.cf** file can be used to customize rules that have set some default values within the appropriate ***.cf*** files (**<install_dir>/spam/rules**).

Do not modify these files as the next upgrade would overwrite your changes.

The **local.cf file** is the place where you can e.g. redefine default scores (for some of technologies) that are set to too low values or not set at all.

In the case you want to create your own rules, create the **<install_dir>/spam/rules/custom/** folder and place these rules here. Again, rules placed to the **rules/** folder would be overwritten. The same applies for editing of the existing rules.

Examples

DKIM

Useful to whitelist Facebook, LinkedIn updates.

Take into account that the **Spam – SpamAssassin – Use DKIM** option has to be enabled "DKIM" functions to work.

Originally, score values from the **rules/25_dkim.cf** file are applied.

Part of the file can look like this:

header DKIM_VERIFIEDeval:check_dkim_verified()

describe DKIM_VERIFIEDDomain Keys: signature passes verification

score DKIM_VERIFIED -0.500

You may want to copy the ***score DKIM_VERIFIED -0.500*** row, paste it into the **local.cf** file and change the value, say to ***-1.000***.

DNSWL

Take into account that the **Spam – SpamAssassin – RBL** has to be enabled "check_rbl_sub" functions to work.

Adding these lines to the **local.cf** file will work:

header __RCVD_IN_DNSWL eval:check_rbl('dnswl-firsttrusted', 'list.dnswl.org.')

header RCVD_IN_DNSWL_LOW eval:check_rbl_sub('dnswl-firsttrusted', '127.0.\d+.1')

describe RCVD_IN_DNSWL_LOW Sender listed at http://www.dnswl.org/, low trust

tflags RCVD_IN_DNSWL_LOW nice net

header RCVD_IN_DNSWL_MED eval:check_rbl_sub('dnswl-firsttrusted', '127.0.\d+.2')

describe RCVD_IN_DNSWL_MED Sender listed at http://www.dnswl.org/, medium trust

tflags RCVD_IN_DNSWL_MED nice net

header RCVD_IN_DNSWL_HI eval:check_rbl_sub('dnswl-firsttrusted', '127.0.\d+.3')

describe RCVD_IN_DNSWL_HI Sender listed at http://www.dnswl.org/, high trust

tflags RCVD_IN_DNSWL_HI nice net

score RCVD_IN_DNSWL_LOW -1

score RCVD_IN_DNSWL_MED -10

score RCVD_IN_DNSWL_HI -100

Spam Queues

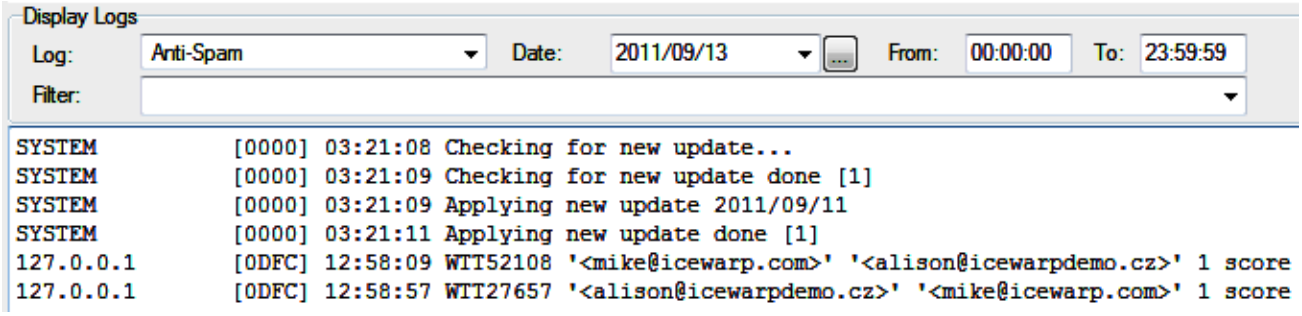
For detailed information on this topic, refer to the **Status – Spam Queues** section.

Logging

If you have set the antispam logging options, you can browse the antispam logs to see what happened to a message, why it was marked as spam, or was not marked as spam.

Enable logging in the **System – Services** node of the administration console. For more information, refer to the **System – Services – General** chapter.

You can view your antispam logs upon the **Status – Logs** node. Select ***Anti-Spam*** and ***Date*** from the appropriate lists. For detailed information, refer to the **Status – Logs** section.



The following is an example of a log entry with an explanation of each field:

Example

127.0.0.1 [07B0] 11:22:54 RSH57851 '<john@doe.com>' '<webmaster@icewarp.com.br>' 1 score 10.00 reason [SpamAssassin=10.00,Bayes=99.99,Body=PE] action SPAM

In this manual, the line is split but within the log screen it would be continuous on one line. The separate fields are described in the table below:

Field	Description
127.0.0.1	This is the IP address that IceWarp Server is connected to send/receive this message.
[07B0]	This is the identifier of the program thread that performed the work.
11:22:54	The timestamp for this log entry.
RSH57851	This is the ID of the message.
'<john@doe.com>'	The user who reportedly sent this message.
'<webmaster@icewarp.com.br>'	The user this message is intended for.
1	The number of recipients this message was intended for.
score 10.00	The spam score this message achieved. *NOTE: This score has a maximum value of 10. The message may have achieved a score higher than 10 but IceWarp Server automatically sets it to 10 if this is the case.*
reason [SpamAssassin=10.00,Bayes=99.99,Body=PE]	SpamAssassin=10.00 – A score from Spamassassin of 10.00. Bayes=99.99 – The probability that this message is spam, according to Bayesian filters. Body=PE: ▪ P – HTML and text parts do not match (see **Reason Codes**). ▪ E – External images in content (see **Reason Codes**).
action SPAM	This is the action taken based on the spam score – in this case SPAM – meaning the message was marked as spam and processed accordingly.

	There are four actions which can be assigned: ▪ SPAM – Message is marked as spam. ▪ QUARANTINE – Message is marked for quarantine processing. ▪ REFUSE – Message is refused. ▪ NONE – Message is accepted.

Reason Codes

The AntiSpam engine issues reason codes when it scores a message as spam, and when it bypasses antispam processing for a message.

There are four logical sets of codes – spam seasons, charset reasons, IceWarp Anti-Spam LIVE reasons and bypass reasons, which are described in the tables below:

Spam Reasons

Code Issued	Reason
P	HTML and text parts do not match
E	External images in content
N	No text part
I	Embedded image in content
B	No body and no subject
R	No intermediary server
S	Message contains a script
F	Spam scored via a filter
K	Spam scored via blacklist keyword
X	Message cannot get to quarantine from any reason (e.g. anti-spam database is not accessible).

Charset Reasons

Code Issued	Reason
F	Charset not allowed
M	Missing charset information

Bypass Reasons

Code Issued	Reason
B	Bypassed because of an entry in the bypass file. This could be sender, recipient, local sender, trusted session, etc.
G	Sender exists in GroupWare address books.
H	Whitelist and blacklist are skipped if the remote side tells us the sender is local, but the session is not authenticated nor comes from a trusted IP. The email is then processed as usually – other rules are applied. It can be turned off only using API console – the ***SpamSkipBypassLocalUntrusted*** variable. *NOTE: So, if this variable is set to **true**, emails from local untrusted users will be checked by antispam (= bypass is skipped). If this variable is set to **false**, messages with a local sender not coming from a trusted connection will be bypassed by antispam.*
K	Words found in whitelist keywords.
L	License is invalid.
M	Spam processing was bypassed because the access mode was set for specific accounts, and this account is not one of them.

O	Message is outgoing.
Q	Local domain senders whitelisted. *NOTE: If you want to whitelist / not whitelist local domain senders, enable/disable this option on the **Anti-Spam – Black & White List** node – **Whitelist tab**.*
R	Sender is listed as a contact in the recipient's IM roster.
S	Message exceeds size threshold for checking.
T	Sender is trusted – the session was authenticated or the sender's IP is set in trusted IPs.
U	If the **Spam** folder or quarantine reports are enabled, senders of all SMTP connections from localhost or from another "friendly" servers in load balanced scenario are compared with the sender specified in the settings of spam/quarantine reports. If match is found, connection is whitelisted and bypass reason U is set.
W	Sender is on whitelist, or a rule was used to ACCEPT the message.
X	Message could not be quarantined for some reasons, e.g. quarantine is not active. (See the **Anti-Spam – General – Other** tab.)
J	Recipient's access mode does not allow to quarantine. (See the **<user> – Policies** tab.)
Z	Local users mode (see the **Anti-Spam – General – Other** tab) is set to ***Do not quarantine / whitelist / blacklist local users.***

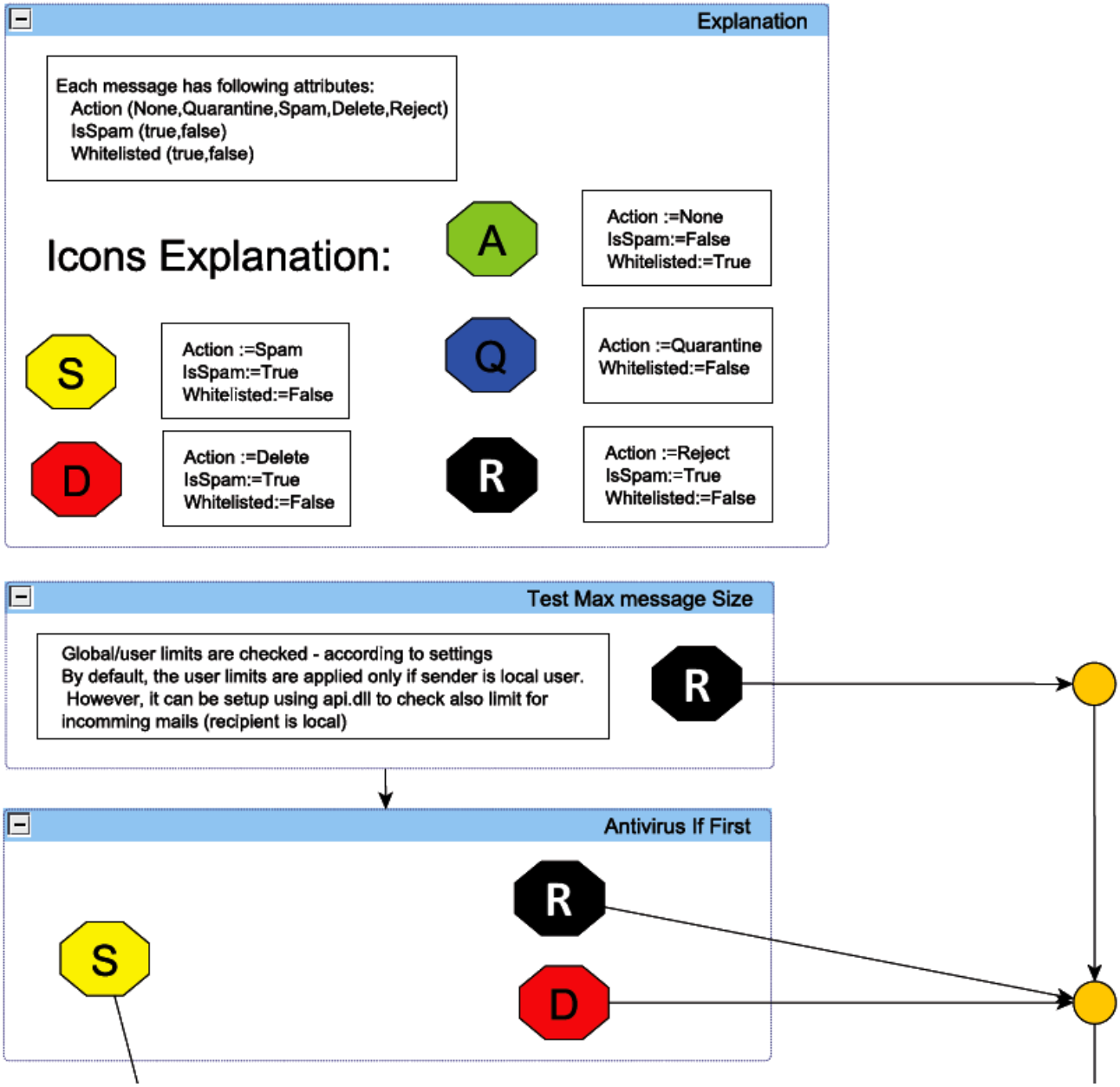
IceWarp Anti-Spam LIVE Reasons – identified as LIVE

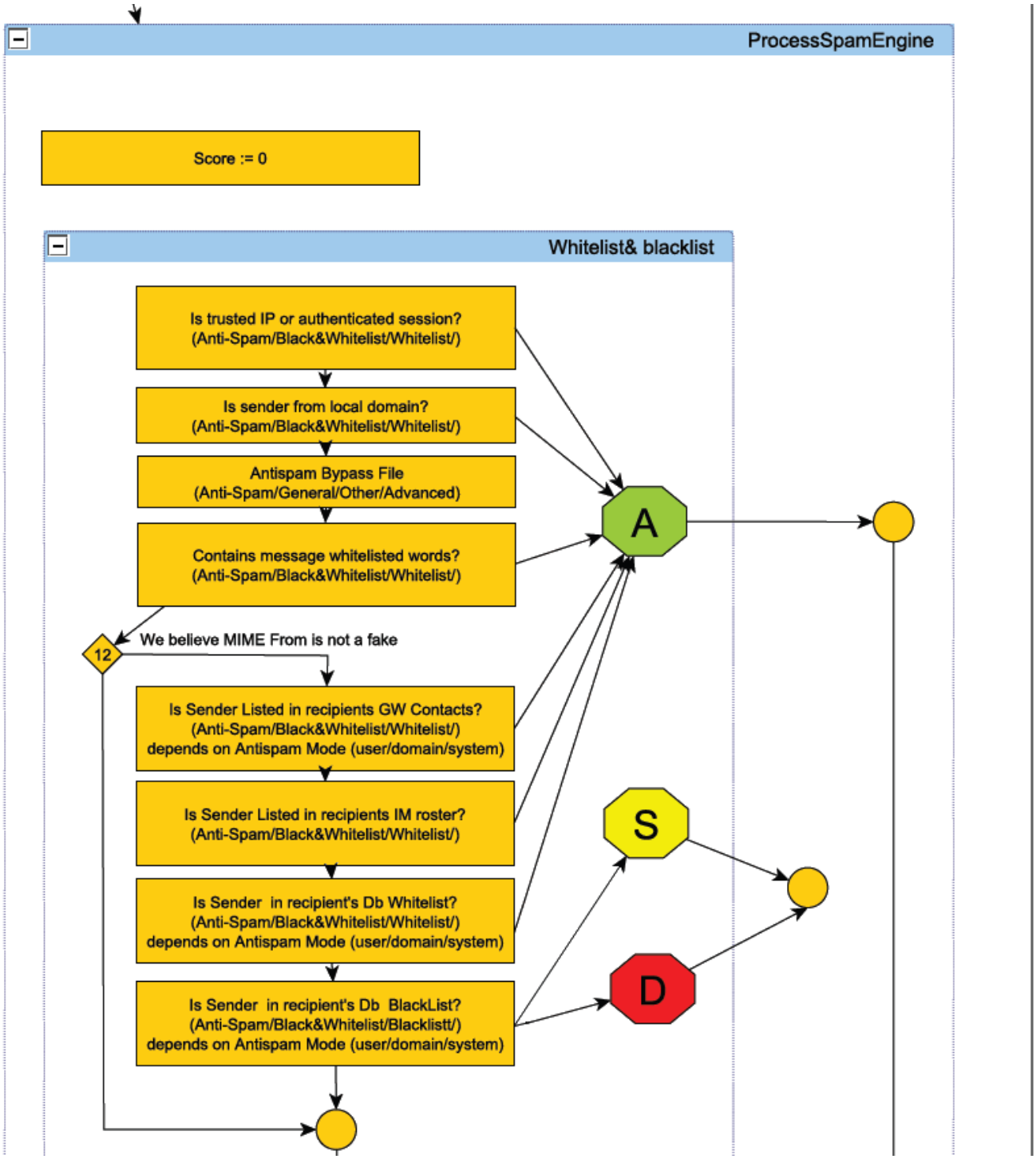
Code Issued	**Reason**
Y	This message is flagged as highly likely spam by the IceWarp Anti-Spam LIVE servers.
H	This message is flagged as highly likely to be a bulk mail.
N	This message is considered genuine.

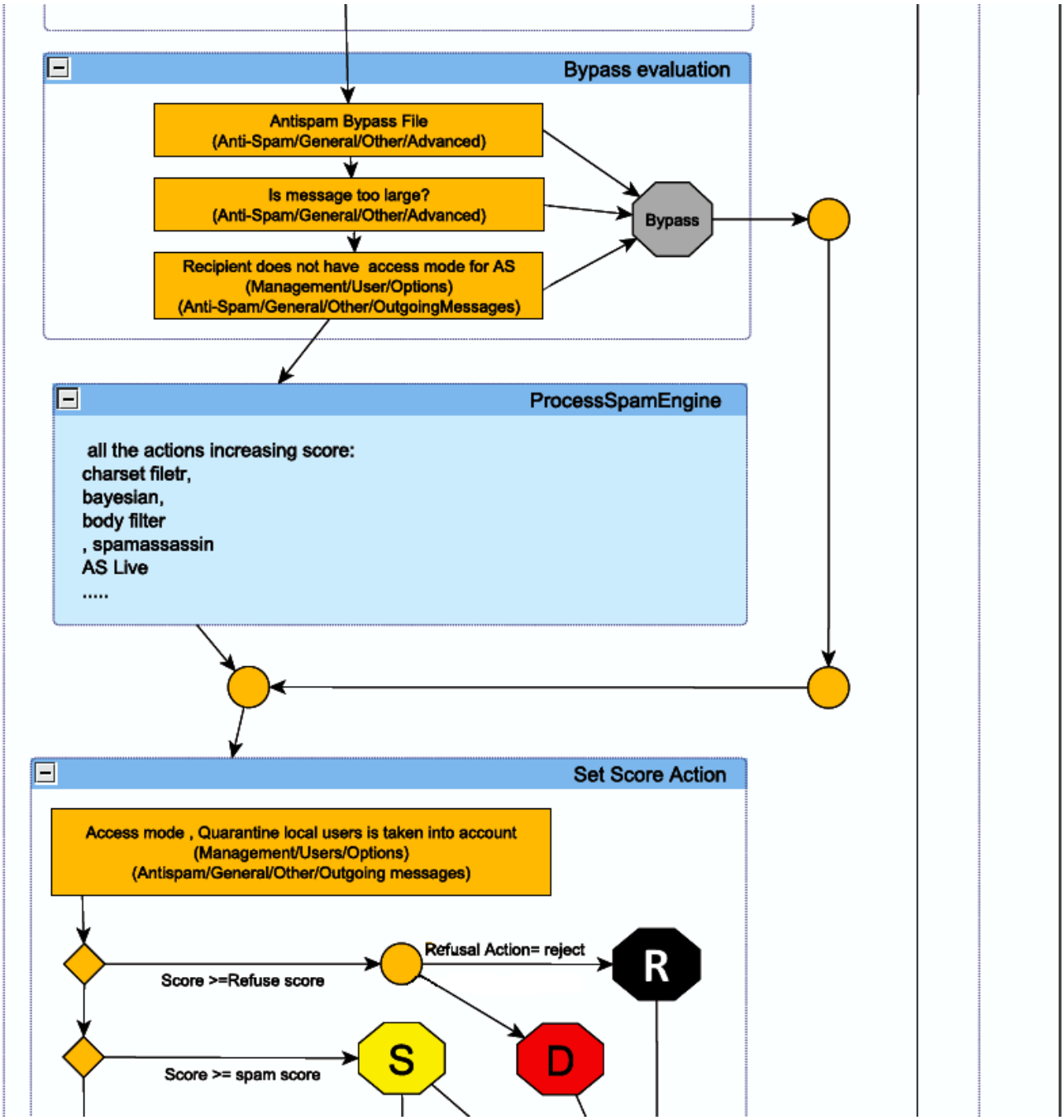
AntiSpam Flowchart

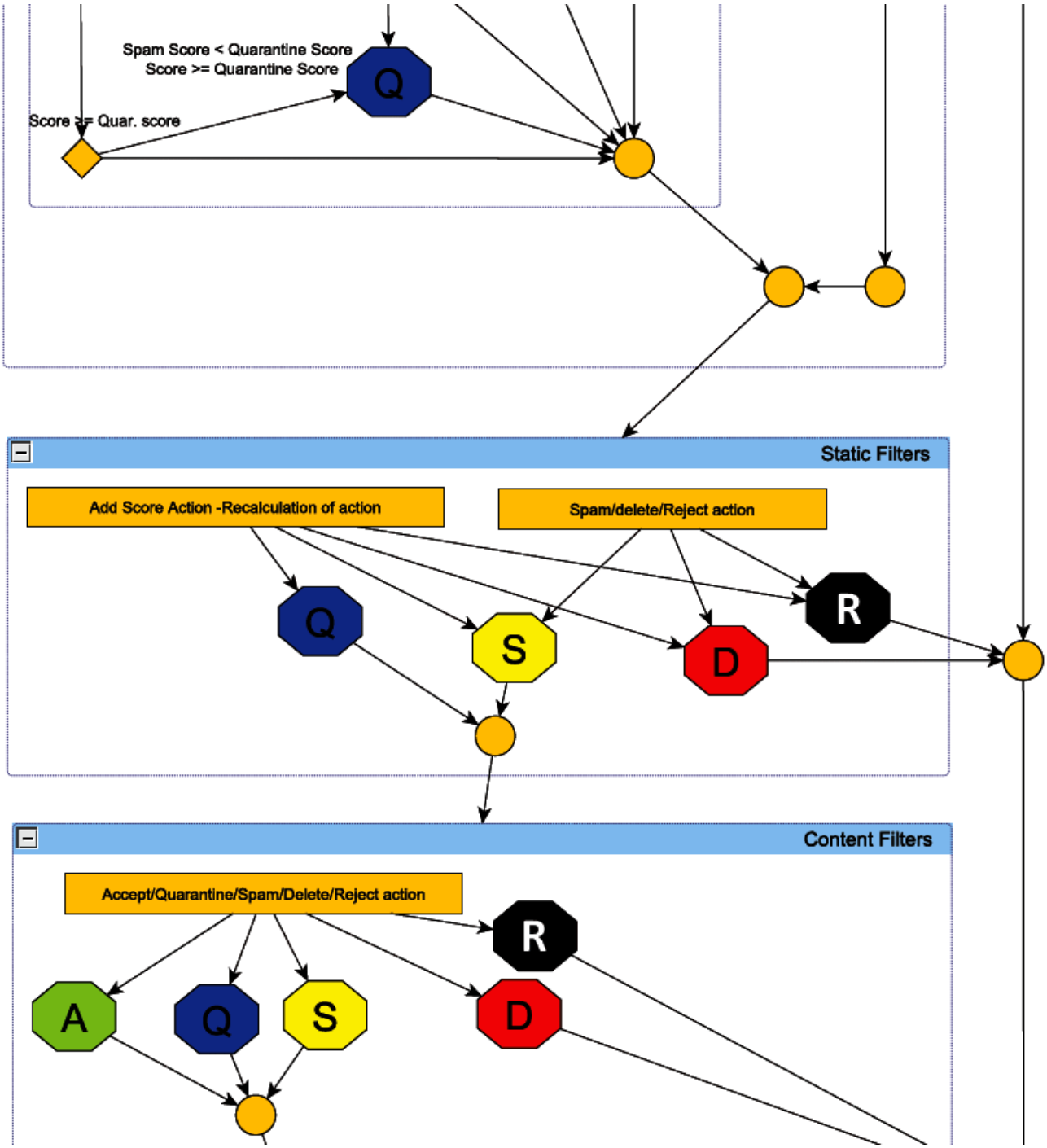
AntiSpam: New Internal Processing

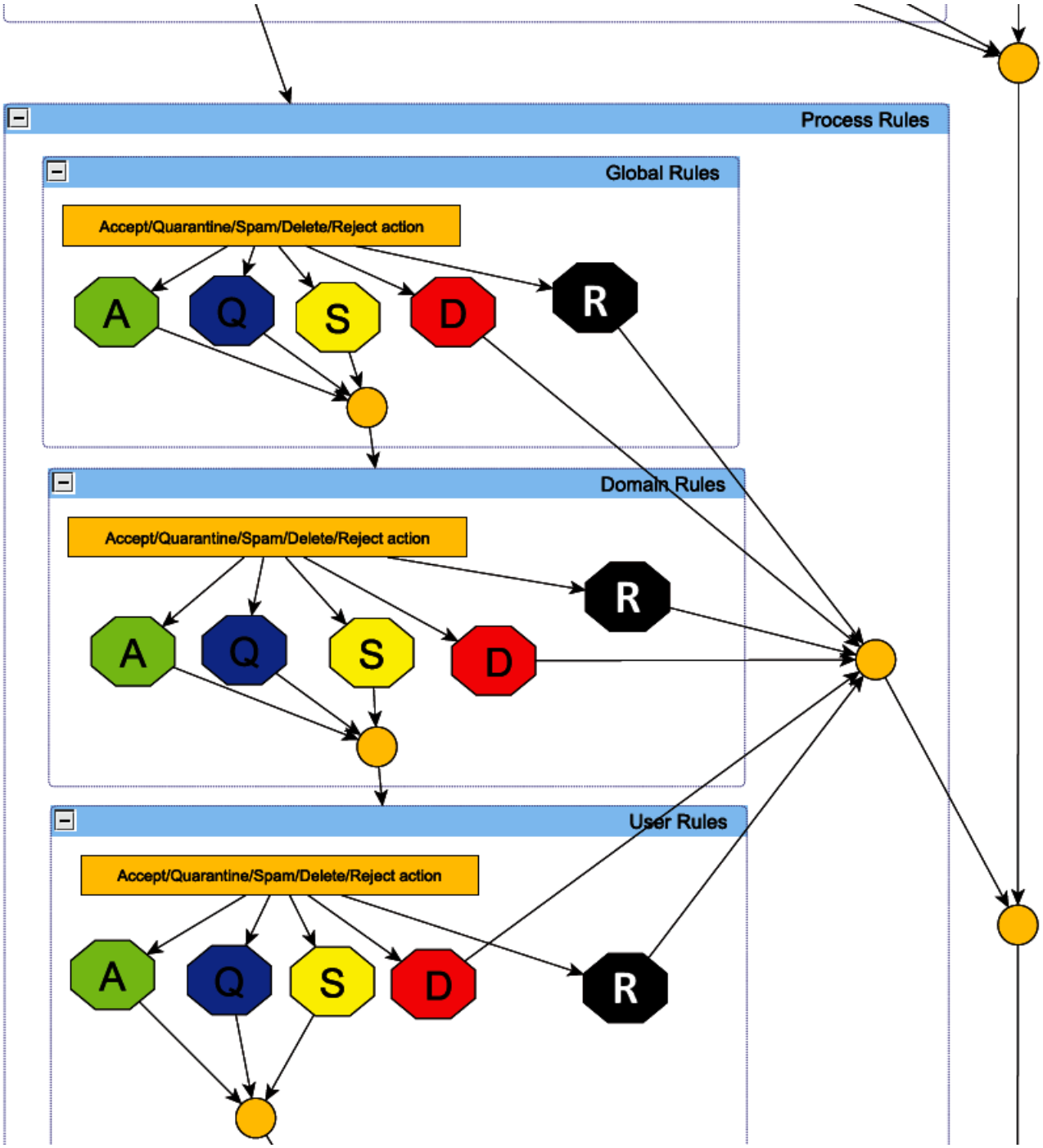
Redesigned Anti-Spam resolves any problems and down-sides of bypasses, access modes, multiple recipients issues, content filter collisions and more.

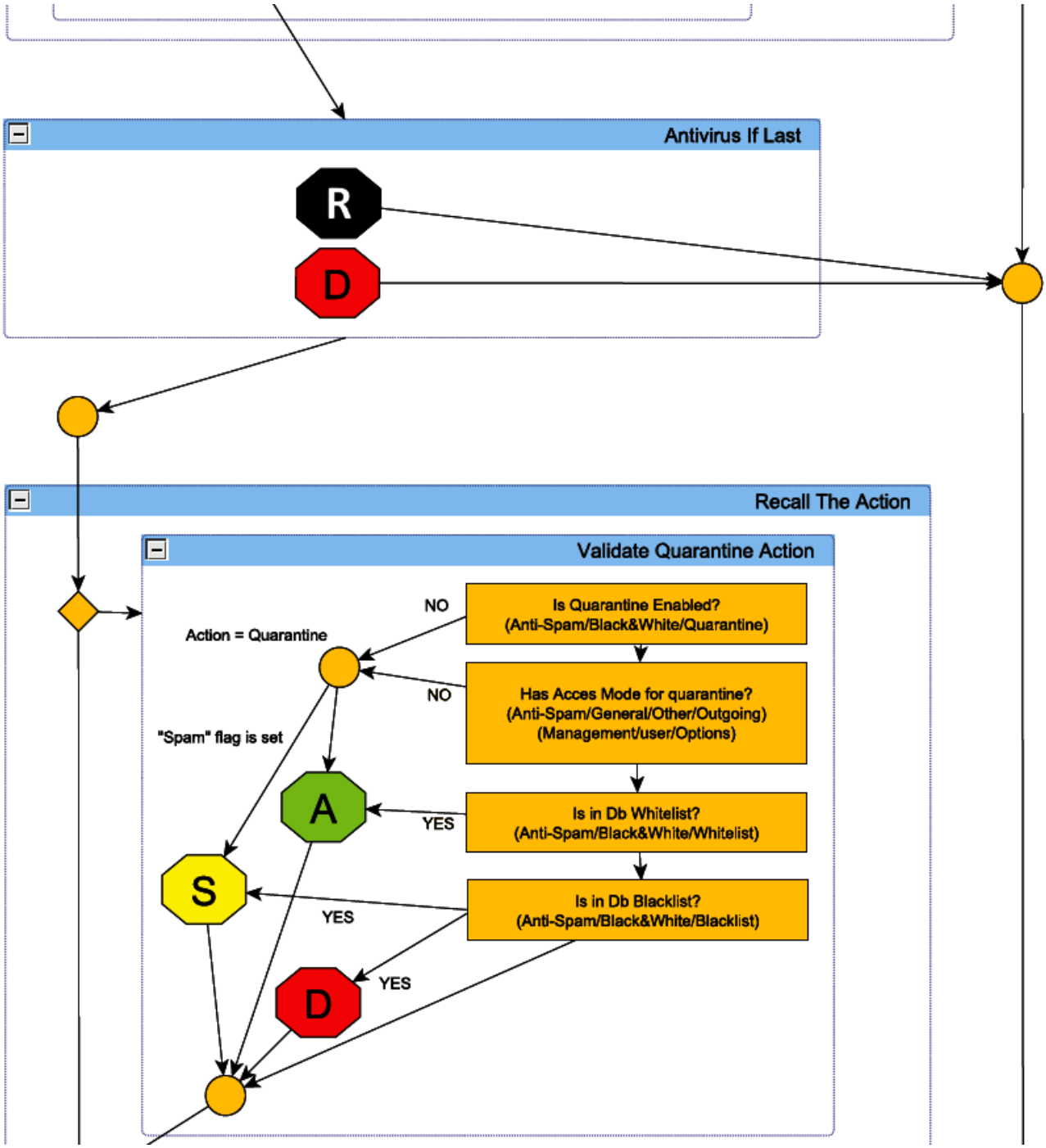


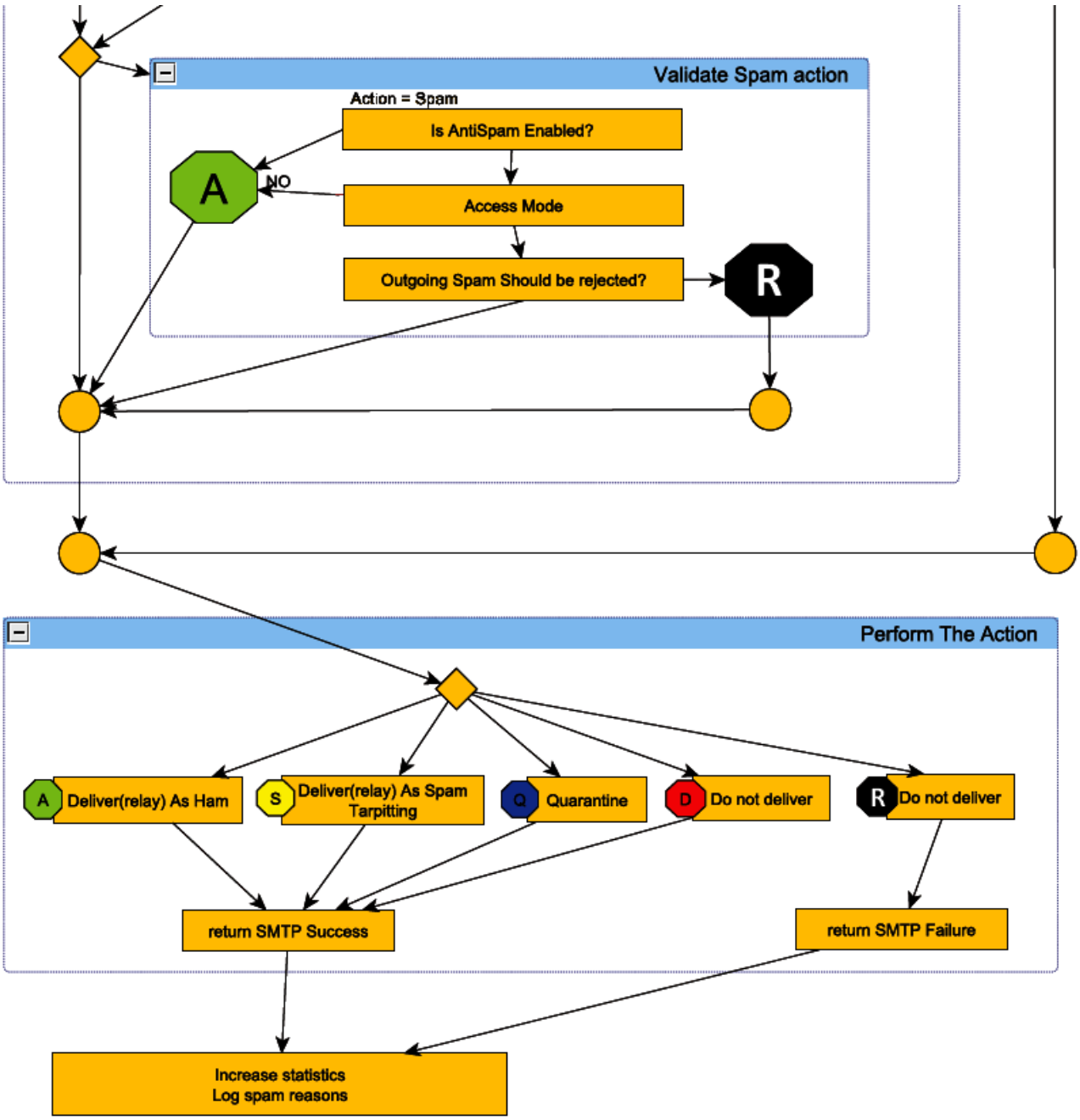

ProcessSpamEngine
Score := 0
Whitelist& blacklist
Is trusted IP or authenticated session?
(Anti-Spam/Black&Whitelist/Whitelist/)
Is sender from local domain?
(Anti-Spam/Black&Whitelist/Whitelist/)
Antispam Bypass File
(Anti-Spam/General/Other/Advanced)
Contains message whitelisted words?
(Anti-Spam/Black&Whitelist/Whitelist/)
A
12
We believe MIME From is not a fake
Is Sender Listed in recipients GW Contacts?
(Anti-Spam/Black&Whitelist/Whitelist/)
depends on Antispam Mode (user/domain/system)
Is Sender Listed in recipients IM roster?
(Anti-Spam/Black&Whitelist/Whitelist/)
S
Is Sender in recipient's Db Whitelist?
(Anti-Spam/Black&Whitelist/Whitelist/)
depends on Antispam Mode (user/domain/system)
Is Sender in recipient's Db BlackList?
(Anti-Spam/Black&Whitelist/Blacklistt/)
depends on Antispam Mode (user/domain/system)
D


Bypass evaluation
Antispam Bypass File
(Anti-Spam/General/Other/Advanced)
Is message too large?
(Anti-Spam/General/Other/Advanced)
Recipient does not have access mode for AS
(Management/User/Options)
(Anti-Spam/General/Other/OutgoingMessages)
Bypass
ProcessSpamEngine
all the actions increasing score:
charset filetr,
bayesian,
body filter
, spamassassin
AS Live
.....
Set Score Action
Access mode , Quarantine local users is taken into account
(Management/Users/Options)
(Antispam/General/Other/Outgoing messages)
Refusal Action= reject
Score >=Refuse score
R
Score >= spam score
S
D


Spam Score < Quarantine Score
Score >= Quarantine Score
Q
Score >= Quar. score
Static Filters
Add Score Action -Recalculation of action
Spam/delete/Reject action
Q
S
D
R
Content Filters
Accept/Quarantine/Spam/Delete/Reject action
R
A
Q
S
D


Process Rules
Global Rules
Accept/Quarantine/Spam/Delete/Reject action
A
Q
S
D
R
Domain Rules
Accept/Quarantine/Spam/Delete/Reject action
A
Q
S
D
R
User Rules
Accept/Quarantine/Spam/Delete/Reject action
A
Q
S
D
R


Antivirus If Last
R
D
Recall The Action
Validate Quarantine Action
NO
Is Quarantine Enabled?
(Anti-Spam/Black&White/Quarantine)
Action = Quarantine
NO
Has Acces Mode for quarantine?
(Anti-Spam/General/Other/Outgoing)
(Management/user/Options)
"Spam" flag is set
A
YES
Is in Db Whitelist?
(Anti-Spam/Black&White/Whitelist)
S
YES
Is in Db Blacklist?
(Anti-Spam/Black&White/Blacklist)
D
YES


Validate Spam action
Action = Spam
Is AntiSpam Enabled?
A
NO
Access Mode
Outgoing Spam Should be rejected?
R
Perform The Action
A
Deliver(relay) As Ham
S
Deliver(relay) As Spam
Tarpitting
Q
Quarantine
D
Do not deliver
R
Do not deliver
return SMTP Success
return SMTP Failure
Increase statistics
Log spam reasons