

A Quick Tutorial on MagicSpam PRO

Once you have activated MagicSpam PRO, you are able to use MagicSpam to its fullest potential. The following sections will show you what you should expect for each page on the MagicSpam interface.

Overview of the MagicSpam PRO Pages

At the top of the MagicSpam PRO extension page, you will see a number of interface component. Below is an overview of what you can find for each interface component.



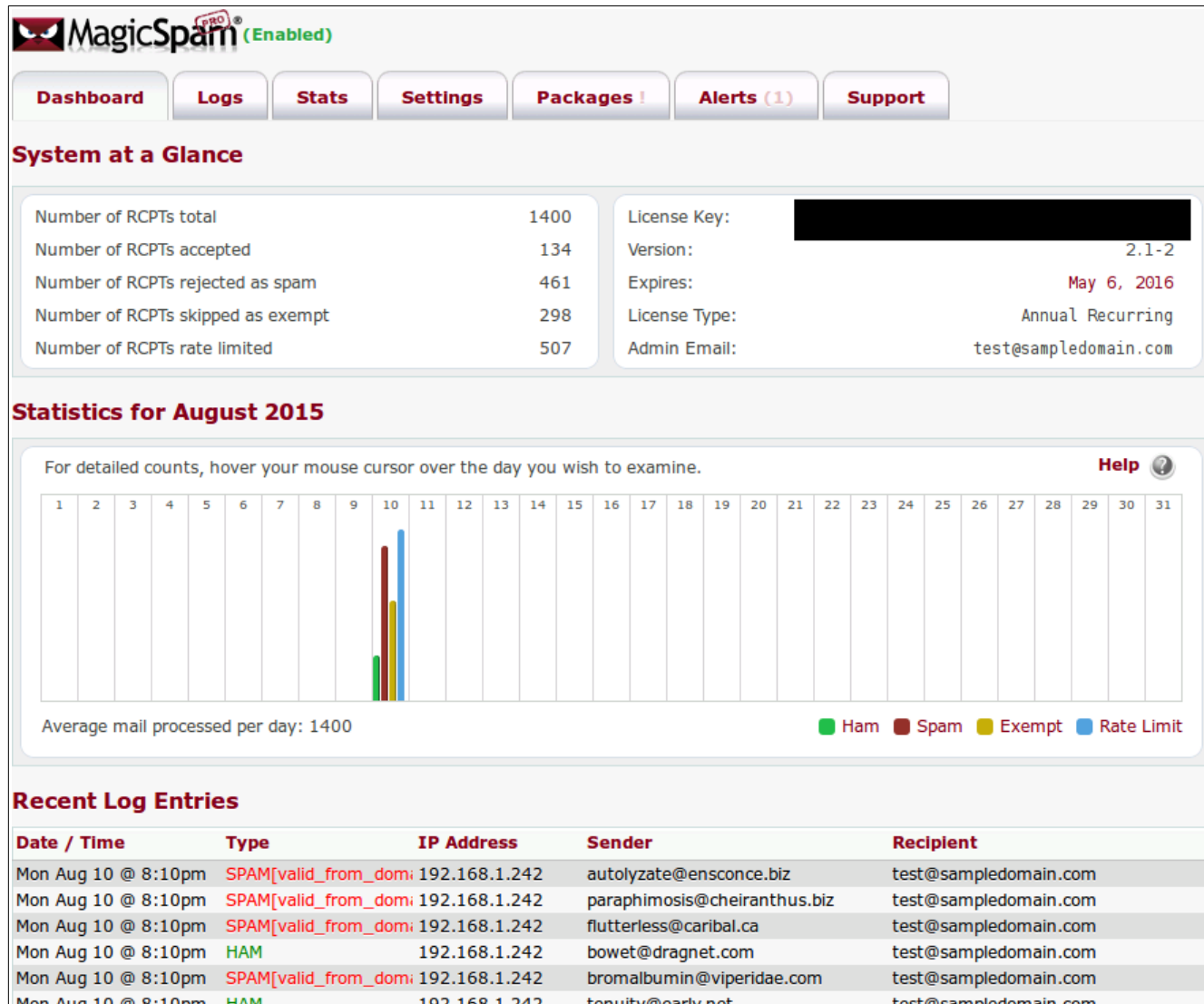
Dashboard

The *Dashboard* is your main MagicSpam extension screen which provides a summary of mail activities on your server. The Dashboard also include monthly statistics of:

- Ham - Messages that were not identified as spam.
- Spam - Messages identified as spam and blocked.
- Exempt - Messages that spam checking was skipped for due to an exemption entry.
- Rate Limited Messages - Messages received from an IP / user who has been rate-limited.

You can hover your mouse cursor over any day in the graph to see details about the statistical counts for each day respectively.


Below is a sample screen shot of what MagicSpam PRO's Dashboard looks like.



Logs

The *Logs* section will provide you with a simple way to search the logs generated by MagicSpam® PRO. It allows you to search based on the following parameters:

- Sender
- Recipient
- IP Address
- Delivery Result (eg. Ham, Spam, etc.)

 **MagicSpam® PRO** (Enabled)

[Dashboard](#) [Logs](#) [Stats](#) [Settings](#) [Packages !](#) [Alerts \(1\)](#) [Support](#)

MagicSpam Logs

Search for detailed information on messages based on sender, recipient, or source IP address information. This is provided as a convenient way to examine the effects of MagicSpam. However, for complete email logs you should still consult with the mail server tools provided by your mail server as other elements could affect email delivery that are outside of MagicSpam's control. (eg. 3rd party filtering, Spam Assassin, or mail server and DNS issues).

Log Search

[Help ?](#)

Sender

Address which sent the email.

Recipient

Address which received the email.

IP Address

IP address of the sender.

Filter by

☒ Limit

Filter and limit search results.

Clear

Search

MagicSpam log location: /var/log/magicspam/

Log retention period: 7 days [Settings](#)

Last log entry: Monday, August 10th 1:11 pm

Total files: 2

Total size (Log / Stats): 266.89 KiB (266.15 KiB / 749 B)

Largest file: mslog (266.15 KiB)

Copyright© 2015 LinuxMagic® Inc., All Rights Reserved.

Underneath the Log Search box is an outline of where MagicSpam's log files are kept on the server. It will show you additional information such as the last entry logged in the file and disk space the log files are occupying.

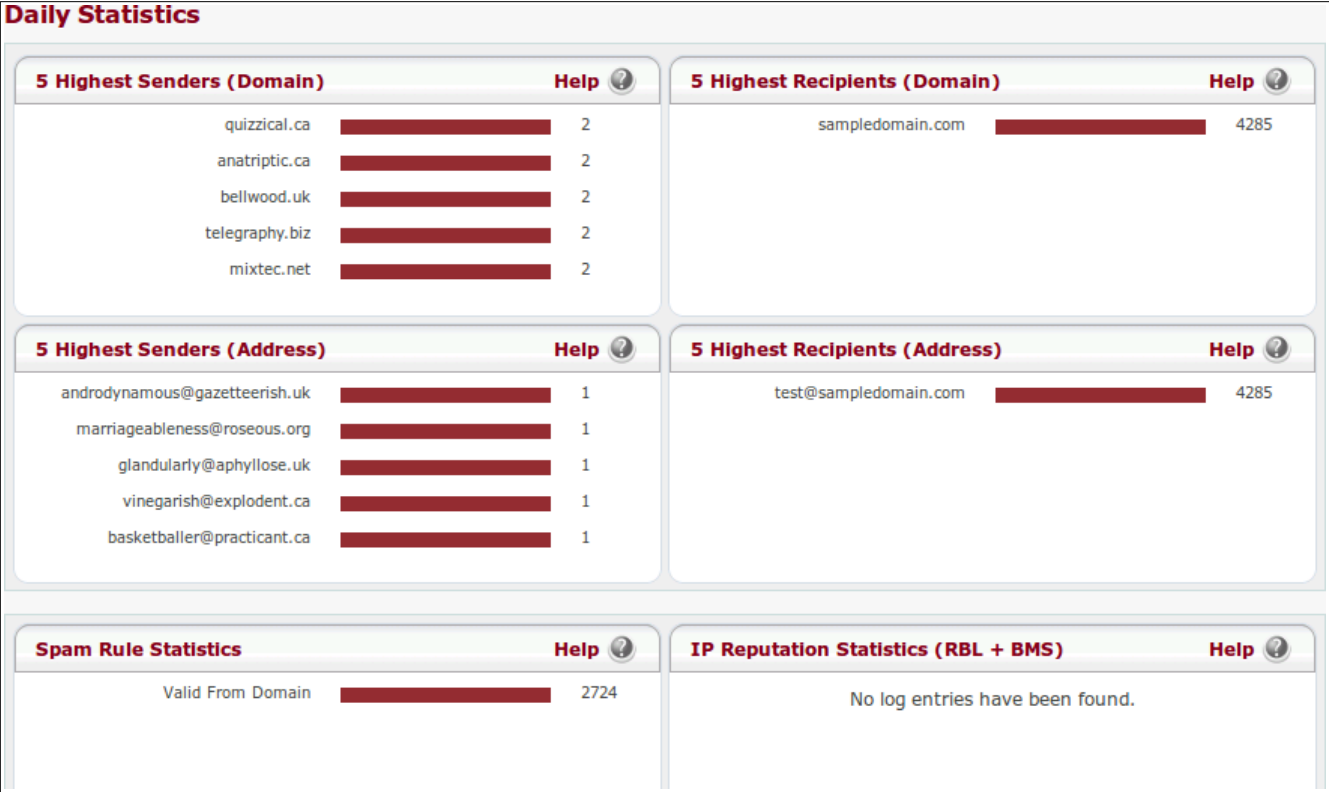
Upon pressing “Search”, you will be able to view the result based on the parameters you provided. This will take you to a new window which will generate the result. You also have the option of downloading the result table as a csv file format – which can be opened and read by most spread sheet programs.

Rows Found: 25 [Click here to download all results as CSV.](#)

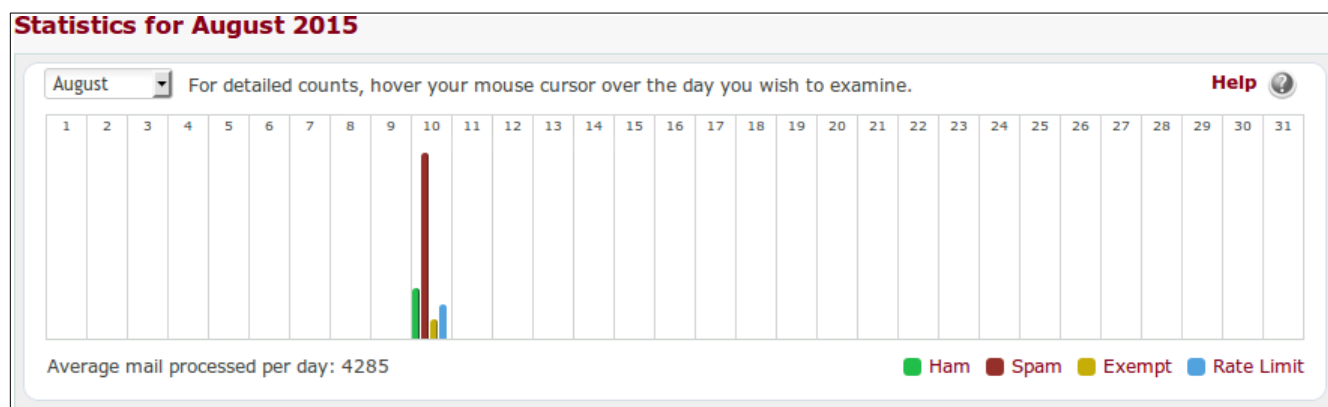
Date / Time	Type	Mua	IP Address	Hostname	Helo	Sender	Recipient
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		gnomological.ca	arthroleura@nonsyllogistic.org	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		neddy.net	heart@guillai.org	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		bacchanalization.ca	untractableness@downess.ca	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		fireable.net	overwilling@intravertebral.net	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		giffgaff.com	superconsequence@defectoscop	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		uncivility.com	trumpet@unclad.ca	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:51 PM	SPAM[valid_from_domain]	no	192.168.1.242		turtleback.biz	wavewise@alcyonacea.biz	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		wharfman.biz	polyparasitic@divinyl.org	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		foremostly.org	anthropozoic@actinopterygious.	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		aduncated.ca	lofty@stretch.uk	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		influxionism.biz	excisor@qorqosaurus.ca	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		pistilline.com	bini@ayubite.uk	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		deducibility.com	semigelatinous@metapepsis.org	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:52 PM	SPAM[valid_from_domain]	no	192.168.1.242		blackcap.com	autolyzate@ensconce.biz	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:53 PM	SPAM[valid_from_domain]	no	192.168.1.242		averruncate.com	paraphimosis@cheiranthus.biz	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:53 PM	SPAM[valid_from_domain]	no	192.168.1.242		preadvise.uk	flutterless@caribal.ca	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:53 PM	SPAM[valid_from_domain]	no	192.168.1.242		postform.ca	bromalbumin@viperidae.com	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:53 PM	SPAM[valid_from_domain]	no	192.168.1.242		noncommunication.uk	rappage@copen.ca	test@sampledomain.com
Monday, Aug 10 2015 @ 8:10:53 PM	SPAM[valid_from_domain]	no	192.168.1.242		answer.com	eeispear@hemibasidiales.org	test@sampledomain.com

Stats

The *Stats* section will allow you to analyze important daily and monthly statistics. Daily statistics will show you the five highest senders and recipients per domain or individual addresses, as well as Spam Rule Statistics and IP Reputation Statistics.



The monthly statistics gives an overview for the current month or for any previous month. This is similar to the statistics displayed in the dashboard, but also gives you the option to see the statistics for previous months.



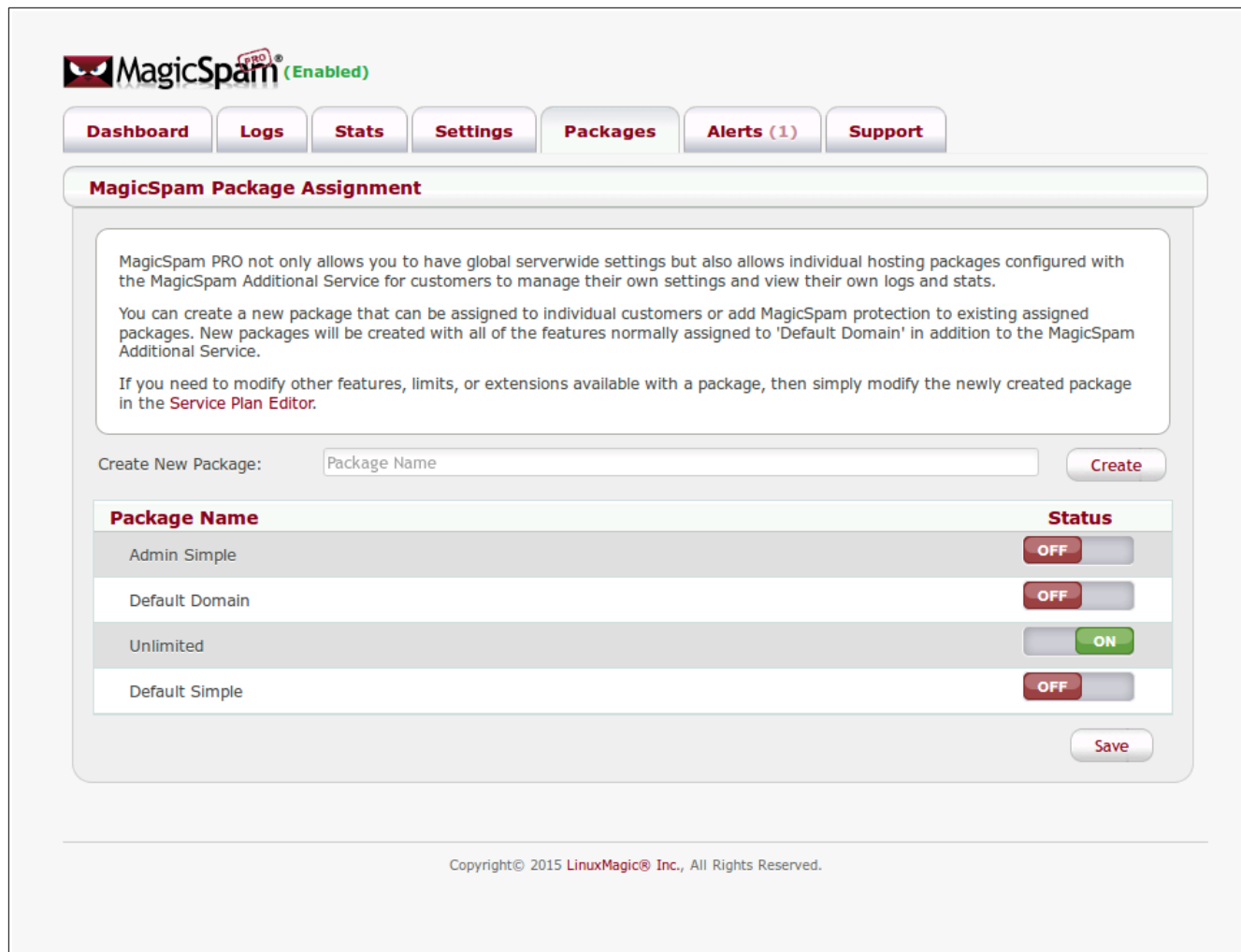
Settings

The *Settings* section allows you to customize your MagicSpam's core settings, server policies, and global protection settings. See [Configuring MagicSpam PRO](#) for more details.

Packages

The *Packages* section allows you to extend MagicSpam PRO to your customers as a value added service. You may add MagicSpam PRO to any service package you currently have or create a new MagicSpam enabled service plan.

The following screen shot example will allow all your customers with an “Unlimited” package to have MagicSpam PRO settings in their own interface.



The screenshot displays the MagicSpam PRO user interface. At the top, the MagicSpam PRO logo is shown with a red 'PRO' badge and the text '(Enabled)'. Below the logo is a navigation bar with buttons for Dashboard, Logs, Stats, Settings, Packages, Alerts (1), and Support. The 'Packages' button is highlighted. The main content area is titled 'MagicSpam Package Assignment'. It contains a text box explaining that MagicSpam PRO allows for global serverwide settings and individual hosting packages. Below this, there is a 'Create New Package' section with a text input field for 'Package Name' and a 'Create' button. A table lists existing packages with their status:

Package Name	Status
Admin Simple	OFF
Default Domain	OFF
Unlimited	ON
Default Simple	OFF

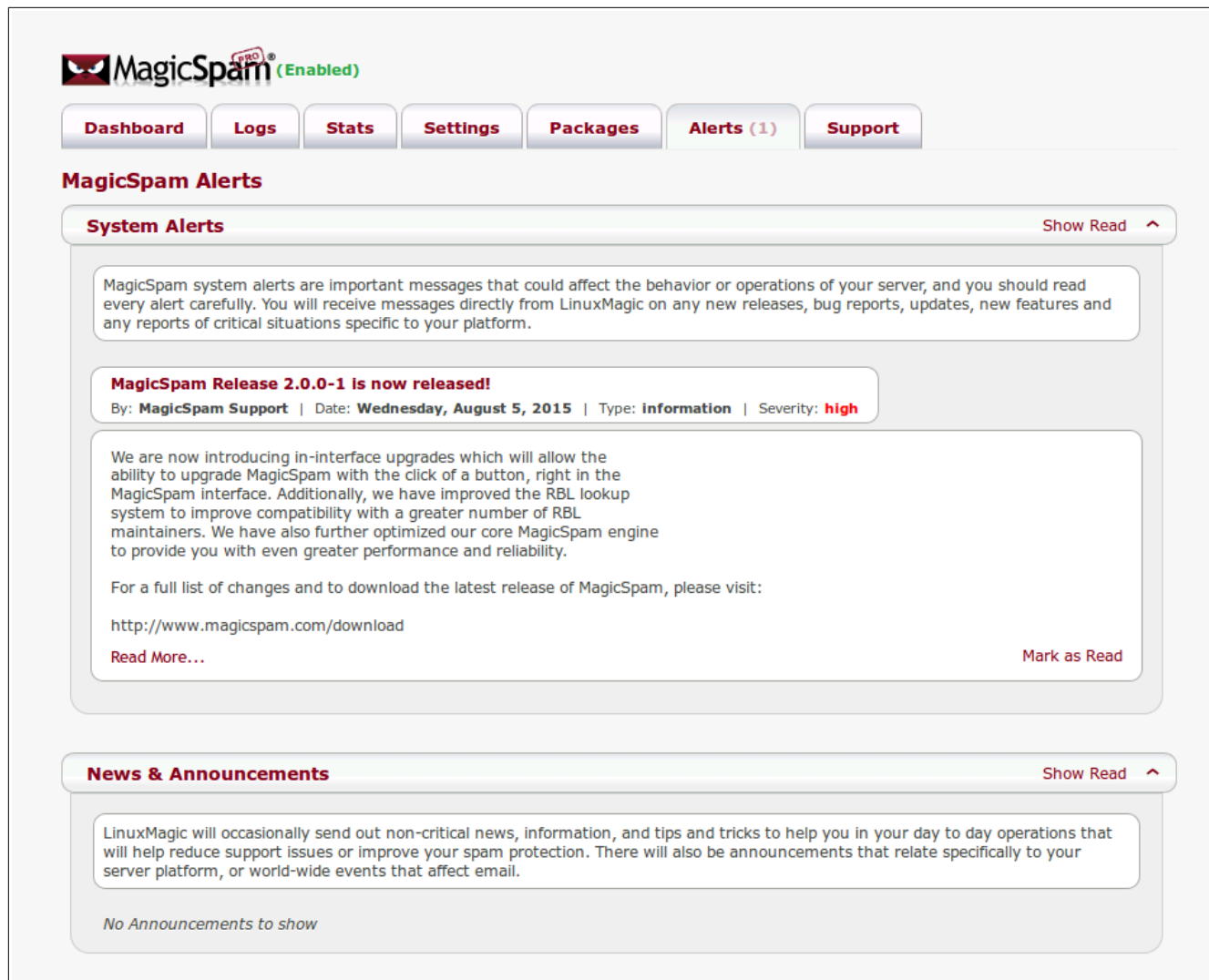
At the bottom right of the table is a 'Save' button. The footer of the interface states: 'Copyright© 2015 LinuxMagic® Inc., All Rights Reserved.'

See [Customer Specific Navigation](#) for more detail.

Alerts

The *Alerts* section notifies you of any news about MagicSpam PRO. Here you can find announcements and additional information from the MagicSpam team, which keeps you informed about MagicSpam PRO updates.

If there is an update available for MagicSpam PRO, you will have the option of upgrading it from this screen as well.



The screenshot displays the MagicSpam PRO interface. At the top, the logo "MagicSpam PRO" is shown with a red "PRO" badge and the word "(Enabled)" in green. Below the logo is a navigation bar with buttons for "Dashboard", "Logs", "Stats", "Settings", "Packages", "Alerts (1)", and "Support". The "Alerts (1)" button is highlighted. The main content area is titled "MagicSpam Alerts" and contains two sections: "System Alerts" and "News & Announcements".

System Alerts (Show Read ^)

MagicSpam system alerts are important messages that could affect the behavior or operations of your server, and you should read every alert carefully. You will receive messages directly from LinuxMagic on any new releases, bug reports, updates, new features and any reports of critical situations specific to your platform.

MagicSpam Release 2.0.0-1 is now released!

By: **MagicSpam Support** | Date: **Wednesday, August 5, 2015** | Type: **information** | Severity: **high**

We are now introducing in-interface upgrades which will allow the ability to upgrade MagicSpam with the click of a button, right in the MagicSpam interface. Additionally, we have improved the RBL lookup system to improve compatibility with a greater number of RBL maintainers. We have also further optimized our core MagicSpam engine to provide you with even greater performance and reliability.

For a full list of changes and to download the latest release of MagicSpam, please visit:

<http://www.magicspam.com/download>

[Read More...](#) [Mark as Read](#)


News & Announcements (Show Read ^)

LinuxMagic will occasionally send out non-critical news, information, and tips and tricks to help you in your day to day operations that will help reduce support issues or improve your spam protection. There will also be announcements that relate specifically to your server platform, or world-wide events that affect email.

No Announcements to show

Support

The *Support* section will provide you information on where to seek assistance if you ever have any issues or questions regarding MagicSpam Pro.

 (Enabled)

[Dashboard](#) [Logs](#) [Stats](#) [Settings](#) [Packages](#) [Alerts \(1\)](#) [Support](#)

MagicSpam Support

MagicSpam is designed to be "Simple to Install, Simple to Use", and we do hope that you should not need any special support. Since you are using a licensed paid version of MagicSpam, support is available via the community support channel and forums.

- [MagicSpam for Plesk](#)
- [Frequently Asked Questions](#)
- [General Discussions and Support](#)

If you have any questions, that is where you want to start to see if your questions are already answered. If you have problems specific to installation, you might want to first check with your hosting provider as they might have non-standard default installations of the operating system and/or control panel or email software for any known issues specific to that provider.

If you have any questions on the spam protection, recommended settings or why a message was blocked or not blocked, the community forums can help you.

As a licensed holder of a paid version, if you have any problems with your license not showing up as active, please contact the reseller or the place you purchased your license. You might also want to look at the FAQ occasionally to see any new tricks and tips, and also make sure that you are getting your updates correctly. Do remember, firewall issues can affect your ability to download new updates regularly, so check your settings page to see that you are getting daily updates.

As well, your hosting provider or reseller may have direct access to our engineering team for advanced support questions.

We truly hope that MagicSpam makes your life easier, and if you have any kind words to share, or any enhancement requests, you might like to also follow us on Twitter [@MagicSpam](#). or even become a [MagicSpam Agent](#) and generate referral fees.

-- MagicSpam Support Team --

PS. If you really understand email, and want to help out the MagicSpam community, we are looking for a few good "spam auditors" and volunteers to join our consumer feedback group.

Copyright© 2015 [LinuxMagic® Inc.](#), All Rights Reserved.

Configuring MagicSpam PRO

MagicSpam PRO has a wide variety of options to choose from. The next section will provide a detailed explanation as to what you can configure for each subsection under the *Settings* page.

System

The *System* section, will provide configuration settings for the Rate Limiter, administrator's email and the number of days that MagicSpam PRO keeps its log entries. The maximum number of days you can keep a log entry file is 60 days. By default (and recommended), MagicSpam PRO will keep its log for seven days.

MagicSpam® PRO will send notifications or updates to the email specified in the Administration Email Address. Please ensure that the administration email address is correct and checked regularly.

The screenshot displays the MagicSpam web interface. At the top, the 'MagicSpam (Enabled)' logo is visible. Below it is a navigation bar with tabs: Dashboard, Logs, Stats, Settings, Packages, Alerts (1), and Support. The 'System' sub-tab is selected under the 'Settings' main tab. The main content area is divided into two sections: 'MagicSpam Protection Status' and 'Options'.

MagicSpam Protection Status

Protection is currently: **Enabled**

When MagicSpam protection is enabled, our IP Reputation and Best Practices rules are applied to your incoming messages and will significantly reduce the amount of spam your users receive.

[Disable Protection](#)

License Key:

Version: 2.1-2

Expires: May 6, 2016

License Type: Annual Recurring

[Enter License Key](#)

Options

Inbound Message Limit:	<input type="text" value="150"/>	Maximum inbound messages permitted.
Inbound Counting Period:	<input type="text" value="5"/>	Time period (in minutes) to count messages towards blocking.
Inbound Expiry Time:	<input type="text" value="360"/>	Expiry time period (in minutes) for an IP to be blocked.
<hr/>		
Outbound Message Limit:	<input type="text" value="150"/>	Maximum outbound messages permitted.
Outbound Counting Period:	<input type="text" value="5"/>	Time period (in minutes) to count messages towards blocking.
Outbound Expiry Time:	<input type="text" value="360"/>	Expiry time period (in minutes) for a user to be blocked
<hr/>		
Administration Email Address:	<input type="text" value="admin@sampledomain.c"/>	Address receives system notices / updates.
Number of days to store logs:	<input type="text" value="7"/>	Logs can be stored on the server for up to 60 days.

The *MagicSpam Protection Status* section shows detailed information about your subscription and status. If your subscription expires, simply press the “Enter License Key” button to update with a new License Key. In normal circumstances this should not be required as subscriptions should automatically renew and update on your server.

The *Options* section allows you to configure both inbound and outbound Rate Limiter settings, which includes:

- Number of messages permitted.
- Time Period for Consideration.
- The Expiry Time of blocked IP addresses.

By clicking on the *Advanced Options* check box, you are given an option to specify a number of parameters to customize MagicSpam's Rate Limiter system.

OptionsHelp

Inbound Message Limit:	<input type="text" value="150"/>	Maximum inbound messages permitted.
Inbound Counting Period:	<input type="text" value="5"/>	Time period (in minutes) to count messages towards blocking.
Inbound Expiry Time:	<input type="text" value="360"/>	Expiry time period (in minutes) for an IP to be blocked.
<hr/>		
Outbound Message Limit:	<input type="text" value="150"/>	Maximum outbound messages permitted.
Outbound Counting Period:	<input type="text" value="5"/>	Time period (in minutes) to count messages towards blocking.
Outbound Expiry Time:	<input type="text" value="360"/>	Expiry time period (in minutes) for a user to be blocked
<hr/>		
Administration Email Address:	<input type="text" value="admin@sampledomain.co.uk"/>	Address receives system notices / updates.
Number of days to store logs:	<input type="text" value="7"/>	Logs can be stored on the server for up to 60 days.

☒ Advanced OptionsSave

The inbound Rate Limiter automatically blocks incoming IP addresses from flooding the server with an excess number of delivery attempts within a set period of time. The outbound Rate Limiter is designed to prevent customer mailboxes (authenticated senders) from sending too many messages within a set period of time in the event of a mailbox compromise or viral activity.

See [Exemptions](#) below for more information related to Rate limiter exemptions.

Exemptions

The *Exemptions* section will allow you to specify IP addresses or email addresses that you wish to bypass MagicSpam's spam protection or even be blocked outright.

Exemptions	
Allows you to specify the senders and IPs which are considered to be exempted, allowed, or blocked. The following categories are configurable:	
Mailboxes with Protection Disabled (1)	▼
Sender From White List (0)	▼
Sender From Black List (0)	▼
Sender IP White List (0)	▼
Sender IP Black List (0)	▼
Per-IP Rate Limiter Whitelist (0)	▼
Per-User Rate Limiter Whitelist (0)	▼

The use of wild card (*) is permitted in most cases, but not recommended. The next section will explain what each exemption does and guide you on when to use each exemption.

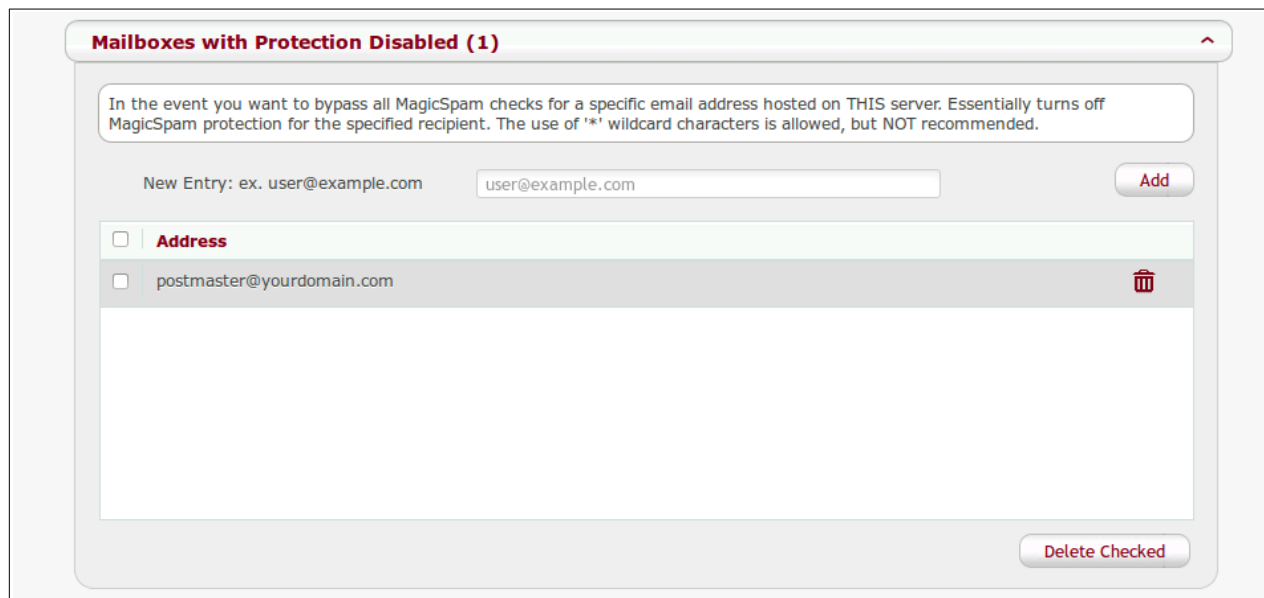
Please note that the email addresses listed under the Exemption lists are still candidates to be Rate Limited unless there is a rate limiter specific exemption entry.

*For more information on bypassing the Rate Limiter,
see the [Per-IP Rate Limiter Whitelist](#)
or [Per-User Rate Limiter Whitelist](#) section below.*

Mailboxes with Protection Disabled

The *Mailboxes with Protection Disabled* section will allow you to specify an email address hosted on YOUR server to fully bypass MagicSpam's check.

For example, if you want to allow “postmaster@yourdomain.com” to be able to receive all messages without MagicSpam intervening, simply add the email “postmaster@yourdomain.com” under the “Mailboxes with Protection Disabled” section.



The screenshot shows a web interface titled "Mailboxes with Protection Disabled (1)". Below the title is a text box explaining the function: "In the event you want to bypass all MagicSpam checks for a specific email address hosted on THIS server. Essentially turns off MagicSpam protection for the specified recipient. The use of '*' wildcard characters is allowed, but NOT recommended." Below this is a form with a label "New Entry: ex. user@example.com", a text input field containing "user@example.com", and an "Add" button. Below the form is a table with a header row containing a checkbox and the text "Address". The table has one data row with a checkbox and the email address "postmaster@yourdomain.com". To the right of the email address is a trash can icon. At the bottom right of the interface is a "Delete Checked" button.

It should be noted that the messages will be classified as EXEMPT[to_whitelist] in your log entry.

Sender From White List

Any email address listed under the *Sender from White List* will be allowed to send messages to any mailbox on the MagicSpam server.

The screen shot example below will allow “alice@anothercompany.com” to send messages to any mailbox on the MagicSpam server.

Sender From White List (1)

SMTP sessions issued with a 'from' argument within this list will be exempt from MagicSpam checks. The use of '*' wildcard characters is supported, but not generally recommended. Please note this matches how the sender identified themselves to your email server. This is different than what you might see in the From: field of the message.

New Entry: ex. user@example.com

<input type="checkbox"/>	Address	
<input type="checkbox"/>	alice@anothercompany.com	

It should be noted that the messages will be classified as EXEMPT[from_whitelist] in your log entry.

Sender From Black List

While not exactly an 'exemption', the email addresses under the *Sender From Black List* section will be instantly blocked by MagicSpam. The *Sender From Black List* section is generally used to prevent unwanted email from specified email addresses.

For example, if you want to block “bob@somebadcompany.com” and automatically classify it as spam, simply add the email in this list.

Sender From Black List (1)

Messages coming from these email addresses will be blocked. Please note this matches how the sender identified themselves to your email server. This is different than what you might see in the From: field of the message.

New Entry: ex. user@example.com

<input type="checkbox"/>	Address	
<input type="checkbox"/>	bob@somebadcompany.com	

When “bob@somebadcompany.com” sends a message to your server, it will show up as SPAM[from_blacklist] in your log entry.

Sender IP White List

The *Sender IP White List* section works the same as the *Sender From White List*, except here you can specify an IP address instead of an email address.



The screenshot shows a window titled "Sender IP White List (1)". Inside, a text box explains: "SMTP sessions from the IP addresses on the following list will be exempt from all MagicSpam checks. Messages which are allowed through due to the sending IP being on this list will show up in the logs with a 'EXEMPT' tag." Below this is a form for adding new entries, with a label "New Entry: ex. 192.168.0.210" and an input field containing "192.168.0.210", followed by an "Add" button. A table below the form has a header row with a checkbox and the label "Address". The first row contains a checkbox, the IP address "192.168.1.123", and a trash icon.

<input type="checkbox"/>	Address	
<input type="checkbox"/>	192.168.1.123	

For example, if you want to allow 192.168.1.123 to send and receive messages, you would add "192.168.1.123" under the Sender IP White List section. Log entries will be classified as EXEMPT[ip_whitelist] when connections are made that match an entry in this list.

Sender IP Black List

The *Sender IP Black List* section works the same as the *Sender From Black List*, except you can specify an IP address instead of an email address. MagicSpam will check the IP address of the message instead of the FROM: field of the message.

If you want to prevent the user from "192.168.1.111" from sending and receiving messages, simply add "192.168.1.111" under the Sender IP Black List section.



The screenshot shows a window titled "Sender IP Black List (1)". Inside, a text box explains: "Messages coming from servers with an IP address on this list will be blocked." Below this is a form for adding new entries, with a label "New Entry: ex. 192.168.0.210" and an input field containing "192.168.0.210", followed by an "Add" button. A table below the form has a header row with a checkbox and the label "Address". The first row contains a checkbox, the IP address "192.168.1.111", and a trash icon.

<input type="checkbox"/>	Address	
<input type="checkbox"/>	192.168.1.111	

Log entries will be classified as SPAM[ip_blacklist].

Per-IP Rate Limiter Whitelist

The *Per-IP Rate Limiter Whitelist* sections allow IP addresses to bypass the inbound Rate Limiter. MagicSpam will still filter messages as spam, ham or exempt. However, this will allow IP addresses in this list to freely send messages without a limitation on the amount within the configured time period. This is commonly useful for cases where you may have a server in your network used to send distribution emails to all of your customers for example.

Per-IP Rate Limiter Whitelist (1)

A list of IP addresses that are excluded from inbound rate limit restrictions.

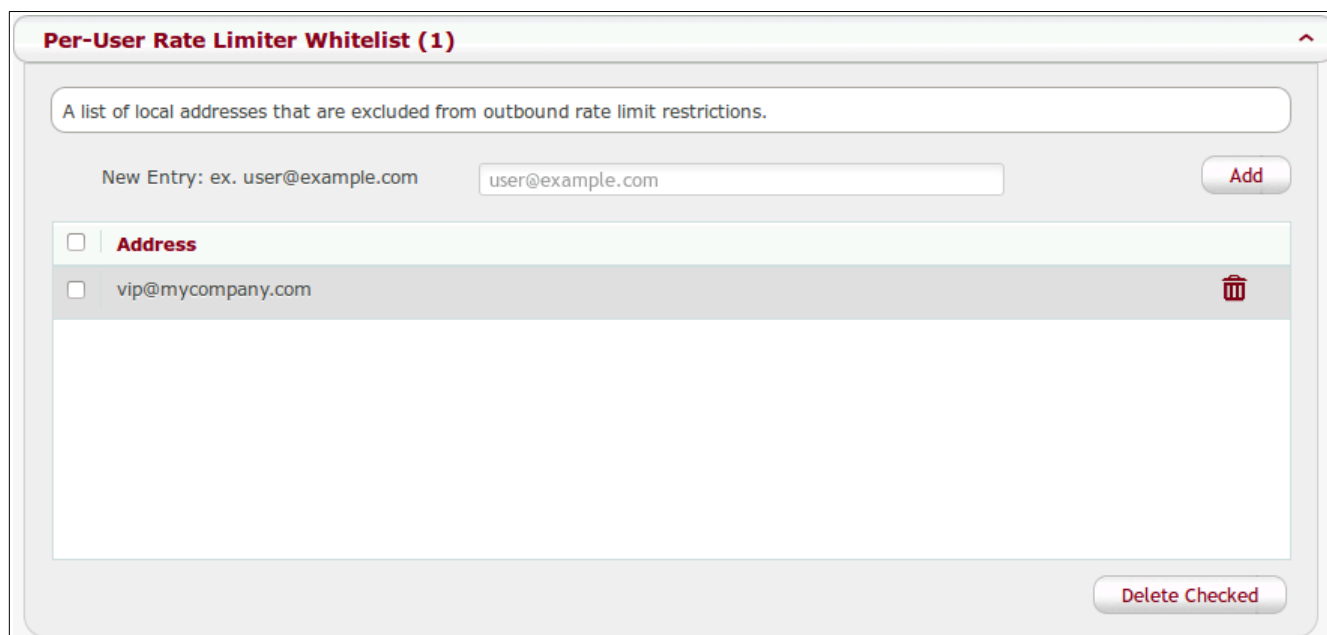
New Entry: ex. 192.168.0.210

<input type="checkbox"/>	Address	
<input type="checkbox"/>	192.168.1.242	

Per-User Rate Limiter Whitelist

The *Per-User Rate Limiter Whitelist* works the same way that the *Per-IP Rate Limiter Whitelist* work, where email addresses specified here will bypass the Per-User Rate Limiter system. This will allow the email address to freely send or receive messages without being blocked by the Rate Limiter system.

The messages will still be classified as spam, ham or exempt in the entry log.



The screenshot shows a web interface titled "Per-User Rate Limiter Whitelist (1)". Below the title is a description: "A list of local addresses that are excluded from outbound rate limit restrictions." There is a text input field with the placeholder "New Entry: ex. user@example.com" and a button labeled "Add". Below this is a table with a header row containing a checkbox and the text "Address". The first row of the table contains a checkbox and the email address "vip@mycompany.com", with a trash icon to its right. At the bottom right of the interface is a button labeled "Delete Checked".

Three-Way Toggle Switch

The following spam policies and rules are available with a three-way switch.



There are three states a rule or policy can be set as:

- On – The policy or rule is strictly enforced and all triggered emails get quarantined
- Flag – The policy or rule is strictly enforced but it will only flag an email as spam
- Off – The policy or rule will not be used to trigger spam hits

Note: You can enable an option to send flagged emails to the spam folder with a checkbox in the 'System' section of the admin panel.

Server Policies

Through MagicSpam server policies you are given the power to customize the server-wide rules which will apply to all customers with a MagicSpam enabled service plan, these policies will dictate how individual users are allowed to change each respective rule in their user panel for MagicSpam. Entries in the 'Exemptions' section will override these policies.

Server Policies

You may configure a number of rules regarding rejecting messages sent by servers which do not follow the accepted best practices for email servers. Improperly configured servers that do not comply with these policies are statistically much more likely to be senders of spam than not.

Server Policy Rule	Status
? Block addresses without domain (e.g. johnny@192.168.1.1) <i>Rule Name: block_ip_in_addr</i>	Recommended <input type="checkbox"/> ON
? Block Mail Servers using COMMON Dynamic/DUL IP space (DYNA REGEX COMMON) <i>Rule Name: check_dynamic_reverse_dns_default</i>	<input type="checkbox"/> OFF
? Block Mail Servers using Dynamic/DUL IP space (DYNA REGEX FULL) <i>Rule Name: check_dynamic_reverse_dns</i>	<input type="checkbox"/> FLAG

When tuning these settings you should take care to only fully enable the 'Recommended' policies and allow your customers with a MagicSpam enabled service plan to further customize their own settings as they desire.

If you are unsure as to what any of the policies do, simply click on the question mark (?) In the left-hand column for an explanation of the rule.

At the bottom of this page you can also check the 'Show Advanced Rejections' box if you wish to create custom rejection messages that will be issued when specific rules are triggered. This can be handy if you wish to give customized information such as your corporate website or contact information specific to your organization – or if you wish to 'localize' the language of rejections specific to your region.

? Block mail from IPv6 addresses that are not authenticated (Experiment...)
Rule Name: block_nonauth_ipv6

☐ OFF

☒ Show advanced rejection message controls

IP Reputation

The IP Reputation section allows you to select from a list of IP Reputation Lists that will be managed by the Blacklist Mastering Systems (BMS). IP Reputation lists are automatically updated databases of known IP addresses of spammers from various sources maintained by a variety of operators, and they are essential to keeping you and your customers' mailboxes spam-free.

The screenshot shows the 'IP Reputation' section of the software interface. At the top, there is a navigation bar with tabs: Dashboard, Logs, Stats, Settings, Packages, Alerts, and Support. Below this is a sub-navigation bar with links: System, Exemptions, Server Policies, IP Reputation (selected), and Rate Limiters. The main heading is 'IP Reputation'. Below the heading, a text box explains that incoming messages will be rejected if they originate from servers found on the enabled lists. A section titled 'BMS® (Blacklist Mastering System) Lists' contains a descriptive text box about the BMS system. Below this is a table with two columns: 'List Name' and 'Status'.

List Name	Status
UCEPROTECT-1 (List Number: 4)	OFF
UCEPROTECT-2 (List Number: 5)	OFF
PSBL (List Number: 13)	ON
SORBS-DUL (List Number: 23)	FLAG

You can click on the question mark (?) icon to the left for the Site URL of the individual list maintainers, or to learn more about the list and the intended use.

Policies set at this level will apply to **all** email traffic coming to your server so you should ensure you only fully enable the safest set of lists, and allow those of your customers with MagicSpam enabled service plans to select any additional reputation lists they wish to enable.

Additionally, you have the ability to utilize any custom RBL (Realtime Blackhole Lists) inside of MagicSpam. If you would like to do this, simply add your list to the RBL menu.

RBL (Realtime Blackhole Lists)

A DNS-based Realtime Blackhole List (RBL) is a list of IP addresses published through DNS for the purposes of identifying source IP addresses associated with Spam activity. From here you can select the public RBL sources you wish to use, or add custom lists to use.

While RBL lists can offer levels of protection against unwanted or unsolicited electronic messages, there is an added overhead for the number of DNS queries made that could negatively affect email delivery services if for example a DNS server has slow response times.

*NOTE: MagicSpam is *not* responsible for maintenance and use of 3rd party RBL services. Please consult the Terms of Use for each RBL service you wish to use to ensure your use of the service is acceptable and/or if service charges may apply.*

?

Add New RBL:

Please enter a name for the new entry

Please enter the host name

Add

List Name	Status	Help ?
<div><div>?</div>The CBL Composite Blocking List (http://cbl.abuseat.org) <small>(RBL-Host: cbl.abuseat.org)</small></div>	<div>OFF</div>	<div></div>

Save

Please note that MagicSpam is **NOT** responsible for maintenance and use of 3rd party RBL services. Please consult the Terms of Use for each RBL service you wish to use to ensure your use of the service is acceptable and/or if service charges may apply.


Rate Limiters

One unique feature of MagicSpam PRO is the ability of limiting traffic for both inbound and outbound mail. The Outbound Rate Limiter is exclusive to MagicSpam PRO.

The Rate Limiter interface will show a list of IP addresses / authenticated senders that are currently blocked from sending or receiving messages. You have the option of unblocking any of those IP addresses / authenticated users listed.

Inbound Rate Limiter

Below is a list of IP addresses that have triggered the rate limiter. Messages will not be accepted from these addresses until the expiry time has been reached, or they are manually unblocked via this table.

<input type="checkbox"/>	IP Address	Time of Block	Expires	
<input type="checkbox"/>	192.168.1.242	Fri, 07 Aug 2015 14:40:59	Fri, 07 Aug 2015 20:40:59	

Unblock Selected

Outbound Authentication Rate Limiter

Below is a list of users that have triggered the rate limiter. Messages will not be accepted from these senders until the expiry time has been reached, or they are manually unblocked via this table.


No entries found.

Customer Specific Rules

Note: Any rules enabled by the server administrator will be enforced within the customer's MagicSpam interface.

MagicSpam PRO features customization at a “per-user” level. This means your customer is free to enable IP reputation lists and server policies which is otherwise disabled at the global level.

Below is a screen shot of the *Dashboard* from a customer's interface.

 **MagicSpam**^{PRO} (Enabled)

Dashboard

Logs

Spam Settings

IP Reputation

Exemptions

System at a Glance

Number of Messages total	0	Number of domains total	1
Number of Messages accepted	0	Number of domains protected	1
Number of Messages spam	0	Number of rate limited addresses	0
Number of Messages exempt	0		

Statistics for September 2015

September ▾ For detailed counts, hover your mouse cursor over the day you wish to examine. Help ?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Average mail processed per day: 0

Ham

Spam

Exempt

Rate Limit


Email Domains

This section displays the current list of email domains presently configured for your account. You can select which email domains you wish to protect with MagicSpam by setting the slider controls below.

Domain	Status
somedomain.com	<div><div></div>ON</div>

Save

The *Logs* page from the customer-level functions the same as the global-level but limited to logs related to just their domains. On this page your customer will also be able to see a list of email addresses within **their** domains that may have triggered the inbound rate limiter system.

 **MagicSpam**^{PRO} (Enabled)

Dashboard

Logs

Spam Settings

IP Reputation

Exemptions

MagicSpam Logs

Search for detailed information on messages based on sender, recipient, or source IP address information. This is provided as a convenient way to examine the effects of MagicSpam. However, for complete email logs you should still consult with the mail server tools provided by your mail server as other elements could affect email delivery that are outside of MagicSpam's control. (eg. 3rd party filtering, Spam Assassin, or mail server and DNS issues).

Log Search

Help ?

Sender

user@example.com

Address which sent the email.

Recipient

user@example.com

Address which received the email.

IP Address

192.168.0.210

IP address of the sender.

Filter by

Detected as Spam

☒ Limit

50

Filter and limit search results.

Clear

Search

*Note: Wildcards in searches are permitted (e.g. *@domain.com).*

Rate Limited Users

Help ?

Below is a list of users that have triggered the rate limiter. Messages will not be accepted from these senders until the expiry time has been reached.

No entries found.

Copyright© 2015 LinuxMagic® Inc., All Rights Reserved.

The screen shot below shows an example of the *Spam Settings* page, which is otherwise known as 'Server Policies' from the administrator's point of view:

Dashboard
Logs
Spam Settings
IP Reputation
Exemptions

Spam Settings

Here you can configure a number of rules to reject messages sent by servers which do not follow the accepted best practices for email servers. Improperly configured servers that do not comply with these policies are statistically much more likely to be senders. Those items listed as **Enforced** have been enabled as policies by the server administrator. Rules may be set to OFF, ON or **FLAG**. If a rule is set to FLAG, messages that trigger the rule will still deliver, but with an altered Subject to indicate the message is potentially spam.

Spam Rule	Status
Block Mail Servers using Dynamic/DUL IP space (DYNA REGEX) <small>Rule Name: check_dynamic_reverse_dns</small>	restricted <input type="checkbox"/> ON
Require Mail Servers to have rDNS configured <small>Rule Name: check_ip_reverse_dns</small>	Enforced <input type="checkbox"/> ON
Block Mail Servers reported as Spam Source (NONDUL REGEX) <small>Rule Name: check_reverse_dns_list</small>	Enforced <input type="checkbox"/> ON
Sending Server must identify itself (HELO) <small>Rule Name: require_helo</small>	Enforced <input type="checkbox"/> ON
Server Identification should be sane (FQDN HELO) <small>Rule Name: valid_helo_domain</small>	Recommended <input type="checkbox"/> ON
Confirm Server Identification Resolves (HELO) <small>Rule Name: resolve_helo_domain</small>	restricted <input type="checkbox"/> FLAG
MAIL FROM: must meet RFC2822 specifications <small>Rule Name: rfc_mail_from</small>	restricted <input type="checkbox"/> FLAG
Strict Email Address Parsing (RFC Compliance) <small>Rule Name: require_full_addr</small>	restricted <input type="checkbox"/> FLAG
Valid FROM domain (A or MX Record) <small>Rule Name: valid_from_domain</small>	Recommended <input type="checkbox"/> OFF
PTR record should be FQDN (Best Practices) <small>Rule Name: valid_ptr</small>	Recommended <input type="checkbox"/> OFF

Restore Recommended
Save

Any Server Policies enabled at the global-level is automatically enforced at the customer-level. The customer is free to customize the Spam Settings to his/her preference.

The same enforcement rule applies for 'IP Reputation'. If the rule is enabled at the global-level, it will be automatically enforced at the customer-level. The customer is free to customize the IP Reputation to his/her preference.

Dashboard
Logs
Spam Settings
IP Reputation
Exemptions

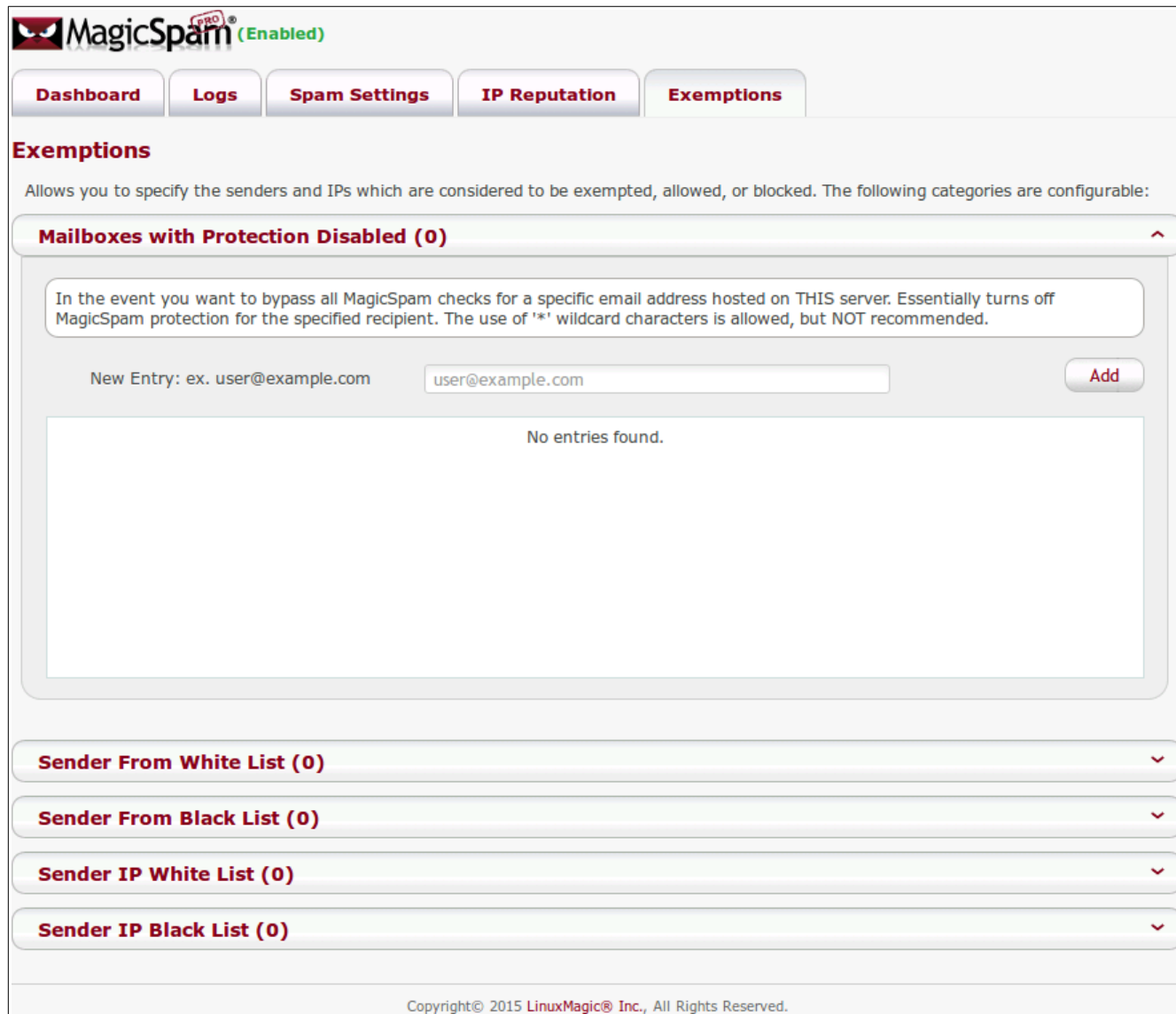
BMS® (Blacklist Mastering System) Lists

BMS, (a highly efficient lookup system) allows your SMTP layer to do real time look-ups against various IP reputation lists which are distributed in the BMS format. By rejecting connections from IP addresses on the lists you select, you significantly reduce inbound attacks, traffic and overhead to your server. This takes effect before RBL checks or server policies, and will help reduce future attacks and possibly even get the email addresses taken off the attackers databases. MagicSpam will reject the connection with a clear message and URL, allowing senders to address their reputation directly with the BMS list maintainer.

List Name	Status
UCEPROTECT-1 <small>(List Number: 4)</small>	<div>OFF</div>
UCEPROTECT-2 <small>(List Number: 5)</small>	<div>OFF</div>
PSBL <small>(List Number: 13)</small>	<div>Enforced</div> <div>ON</div>
SORBS-DUL <small>(List Number: 23)</small>	<div>restricted</div> <div>ON</div>
MIPSpace-all <small>(List Number: 35)</small>	<div>restricted</div> <div>ON</div>
MIPSpace-worst <small>(List Number: 40)</small>	<div>restricted</div> <div>ON</div>
MIPSpace-poor <small>(List Number: 41)</small>	<div>restricted</div> <div>ON</div>
MIPSpace-pros <small>(List Number: 42)</small>	<div>restricted</div> <div>FLAG</div>
RATS-Dyna <small>(List Number: 36)</small>	<div>Recommended</div> <div>ON</div>
RATS-NOPTR <small>(List Number: 37)</small>	<div>Recommended</div> <div>ON</div>
RATS-Spam <small>(List Number: 38)</small>	<div>Enforced</div> <div>ON</div>

Restore Recommended
Save

Like the administrator interface, customers are able to add exemptions under the *Exemptions* page to control their own white list and black list.



MagicSpam ^{PRO} (Enabled)

[Dashboard](#) [Logs](#) [Spam Settings](#) [IP Reputation](#) [Exemptions](#)

Exemptions

Allows you to specify the senders and IPs which are considered to be exempted, allowed, or blocked. The following categories are configurable:

Mailboxes with Protection Disabled (0)

In the event you want to bypass all MagicSpam checks for a specific email address hosted on THIS server. Essentially turns off MagicSpam protection for the specified recipient. The use of '*' wildcard characters is allowed, but NOT recommended.

New Entry: ex. user@example.com [Add](#)

No entries found.

Sender From White List (0)

Sender From Black List (0)

Sender IP White List (0)

Sender IP Black List (0)

Copyright© 2015 LinuxMagic® Inc., All Rights Reserved.

Note: The Rate-Limiter system can only be configured at the global-level. Customers do not have the option of configuring the Rate-Limiter settings.