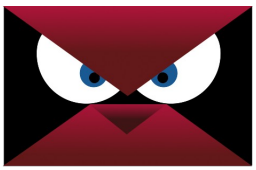


MagicSpam®

*The best antispam for your mail server.*

# MagicSpam PRO for WHM/cPanel Installation and Usage Guide

Thank you for your purchase of MagicSpam PRO for WHM/cPanel! This document is intended to outline the installation process and guide you through the first steps for implementing server wide protection as well as setting up support for MagicSpam to be managed by customers subscribing to select Hosting packages.

Please note that this guide is specifically designed for the PRO for WHM/cPanel edition of MagicSpam and is not intended to b used with other release editions. What is the difference? The PRO edition is designed specifically to allow you to allocated MagicSpam protection based on a 'value add' proposition. Of course, you also have the option of running server wide protection as well.

## Requirements

- Possess an active license key for 'MagicSpam PRO for WHM/cPanel'.
- Working cPanel server to perform installation on.
- Administration (root) access to said server
- 1 GB hard drive space in /var for updates and profiling databases

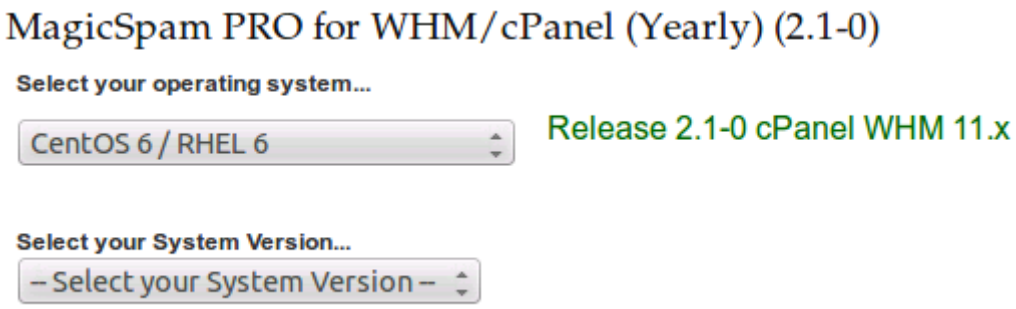
MagicSpam does not require any additional CPU or Memory resources in order to provide protection, and will in most cases reduce server overhead as a result of the unique approach used to reject spam.

## Step 1 – Downloading

Before starting, you will need to download the appropriate MagicSpam package from the following URL:

http://www.magicspam.com/download

Simply enter your License Key (provided on your receipt). You will be presented with a menu similar to the following for selecting the appropriate package (Make sure the package name starts with 'magicspampro-cpanel').




Select your operating system from the drop down menu and click the resulting download link from the right hand side. Once the download is complete, transfer the file to your cPanel server using any method you prefer (eg: FTP, SFTP, or the cPanel File manager).

## Step 2 – Installation

Before beginning this step, ensure you are logged in as a use with root privileges on the cPanel server. This is required in order to successfully install the MagicSpam PRO for cPanel/WHM package.

Open a terminal session and enter the following command (ensure that you replace the directory location and filename to be accurate):

```
rpm -ivh /path/to/uploaded/package
```

This will begin the installation process. Please note – if you are upgrading from an older version of MagicSpam PRO, you can use the command:

```
rpm -Uvh /path/to/uploaded/package
```

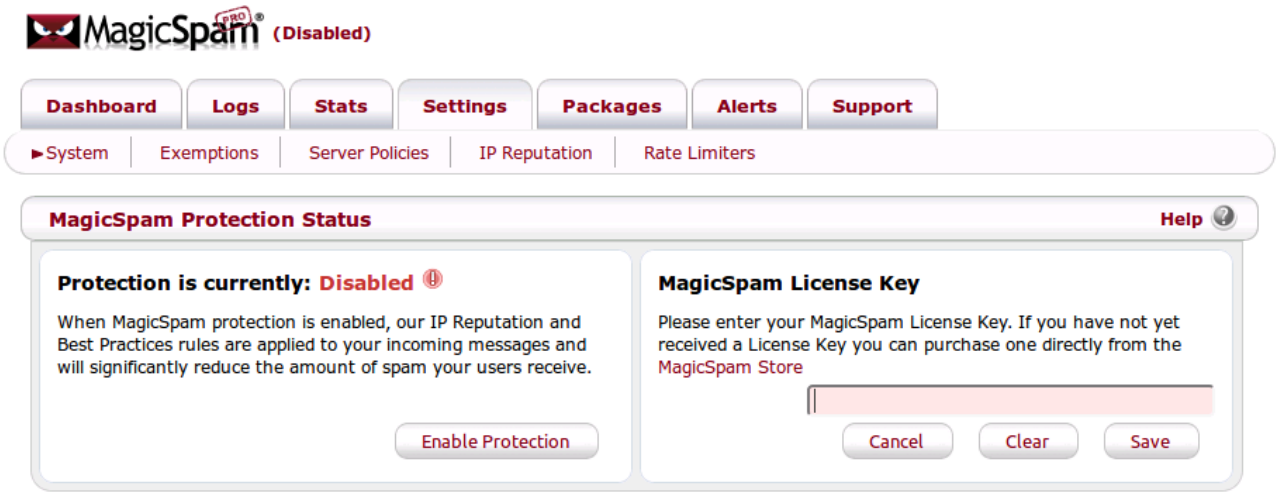
Allow a few moments for the installation to complete. When complete, you will be returned to the command prompt with the following message:

```
================================
Installation complete! Your next
step is to point a web browser to
your WHM interface and launch
Plugins / MagicSpam to configure!
```

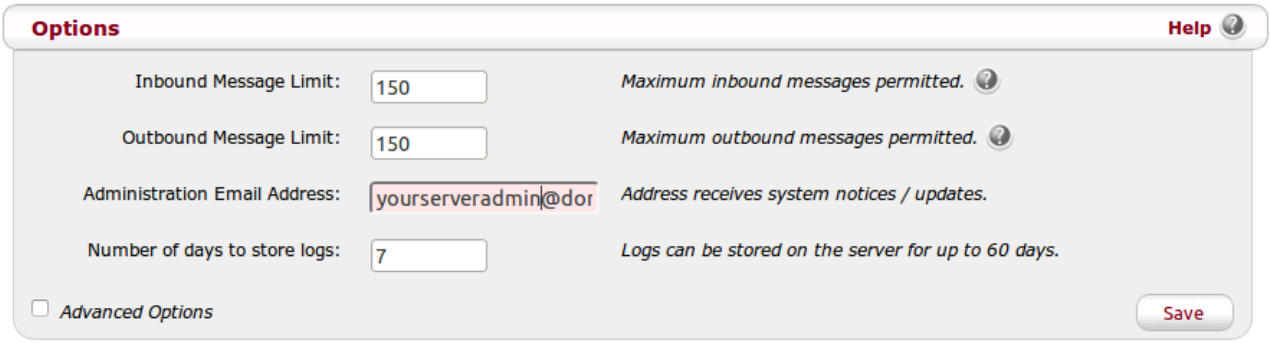
# Step 3 – Initial Configuration

At this stage MagicSpam PRO for WHM/cPanel will be installed and accessible in the WHM interface. Log in to your WHM panel. Once logged in, click on “Plugins” , then “MagicSpam” You will be presented with the following screen:




You can enter your license key in the entry box then click 'Save' to register your installation.

Right below the License Key input is a section for setting the email address to be used for system notifications. This address will only be contacted for critical situations such as errors in processing spam definition updates, license updates, or any other conditions found that could cause MagicSpam to become inoperable. The package itself will attempt to auto fill this information based on the server administrator email, but if you need to change this to a different address, simply enter the new address and click Save.

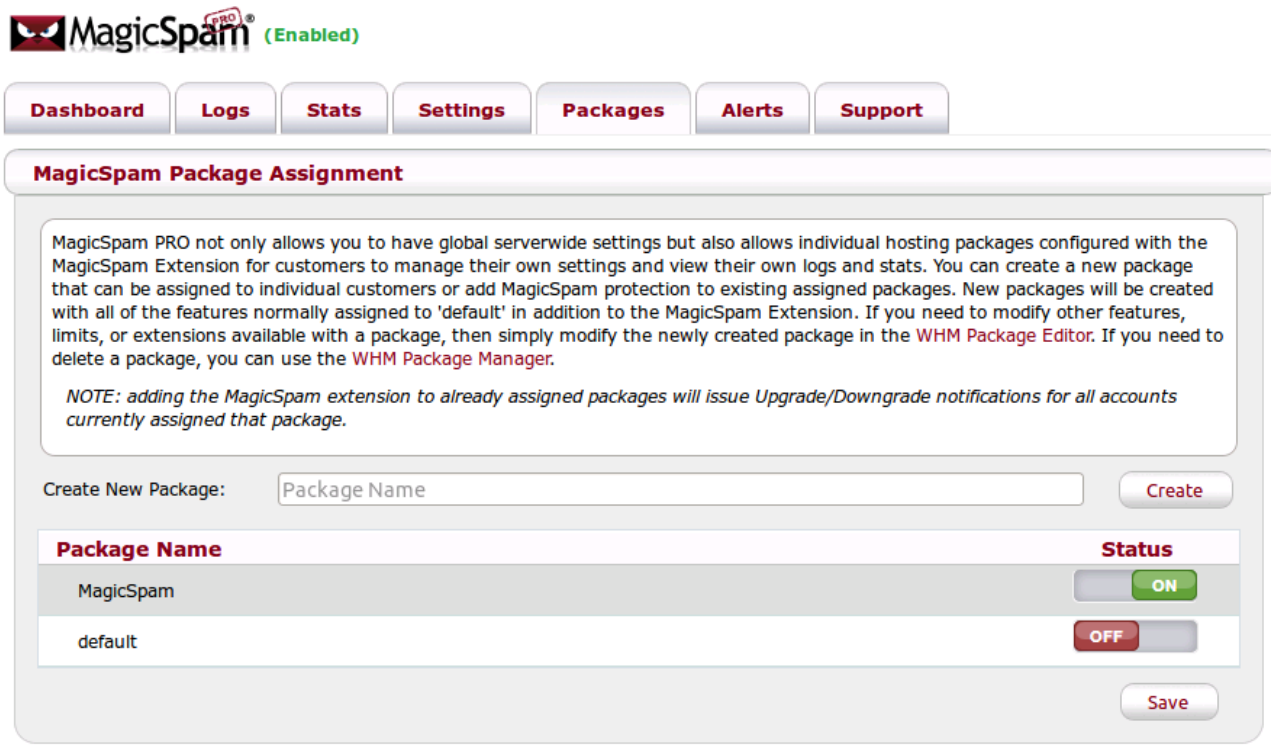



Once your license and administration email address are saved, you can click on 'Enable Protection'. Enabling MagicSpam will also launch the first set of spam definition updates in the background.

Once enabled, you can then click on 'Server Policies' and 'IP Reputation' to review the initial 'global' spam protection settings that you wish to apply to your server. These settings will affect **all** email being delivered to your server. The MagicSpam installation package will enable those rules and reputation lists that have proven as effective and safe.

Moving past the global protection policies, you can also use MagicSpam PRO as a value add option for customers. Click on 'Packages'. From here you can assign the MagicSpam resource to existing Hosting packages, or alternatively create a new Hosting package with the MagicSpam resource enabled.

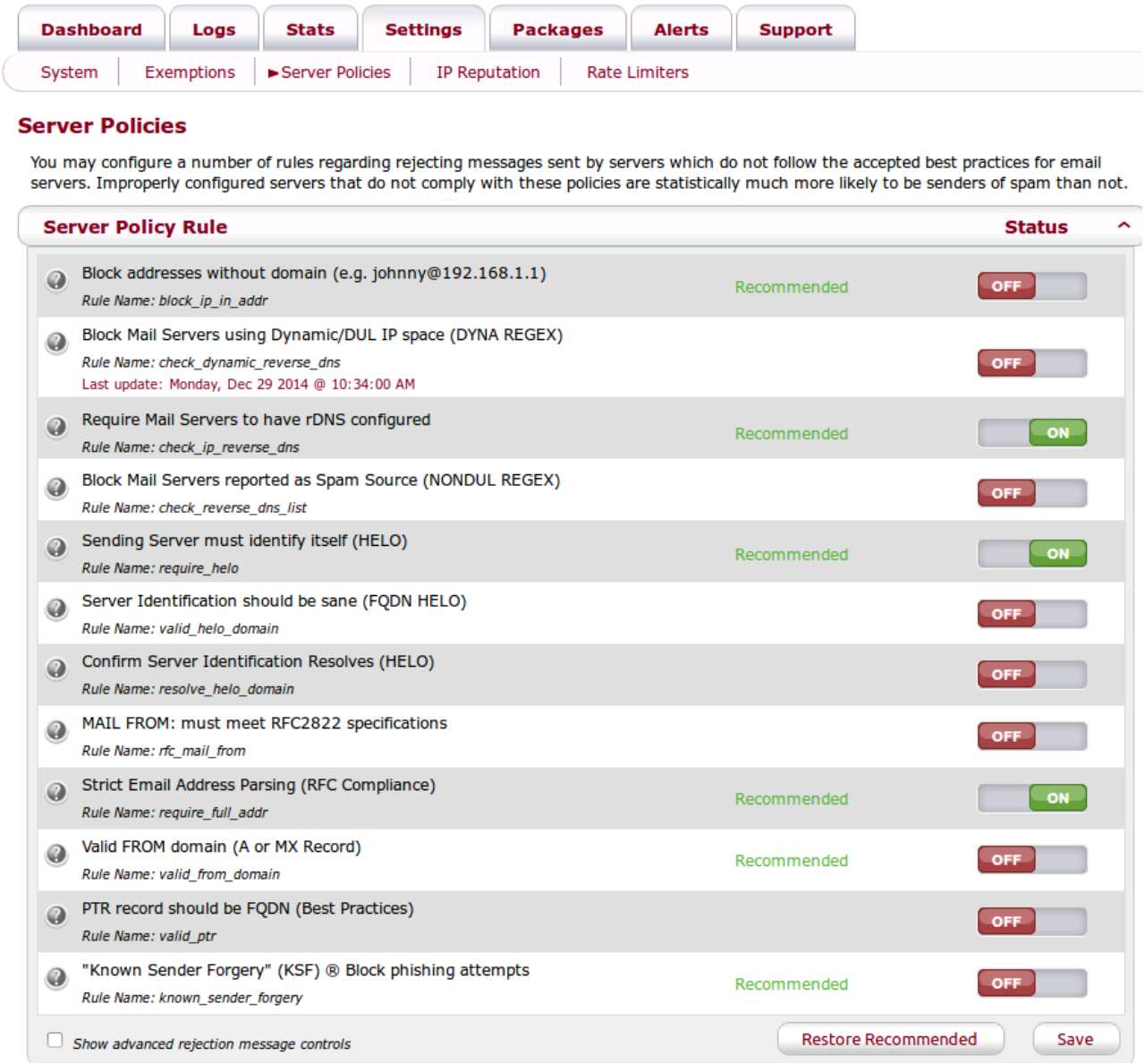



When a customer has been assigned a package that includes MagicSpam protection, all email domains associated with their account will be granted an additional layer of MagicSpam protection. They will also have a new MagicSpam icon available to them in their cPanel interface. This icon will allow them to control the additional rules and policies that they wish to have enabled, control their own white list and black list entries, as well as allow them to view and search their own logs and statistics of protection. They will also be given the option of selectively enabling or disabling protection on individual email domains that they operate on your server.

# Step 4 – Extended Configuration

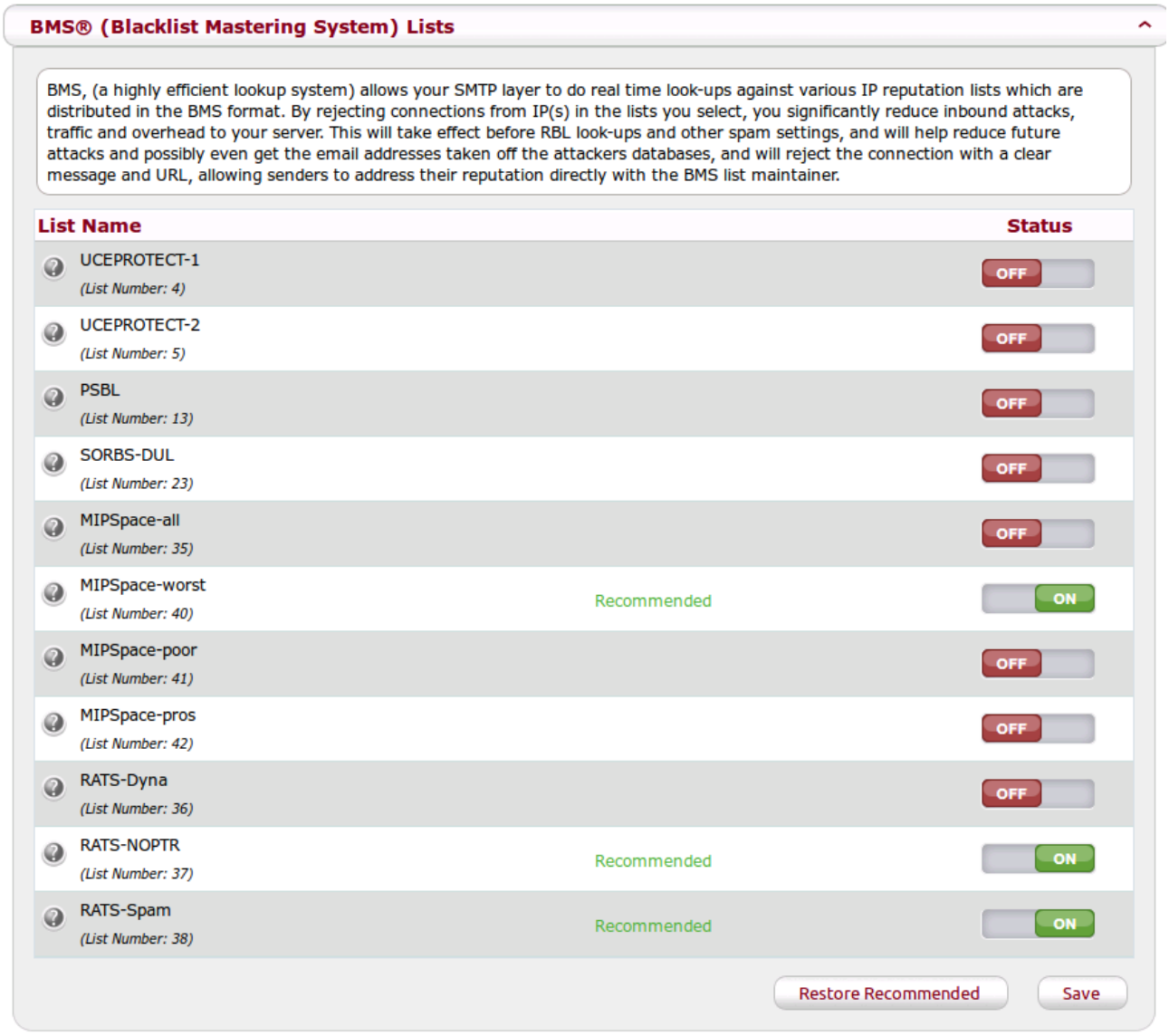
When first installed MagicSpam PRO will enable a default set of recommended Server Policies and IP reputation lists for use at the Global level. You do however have the option of tailoring this protection as you need. Click on “Settings” then “Server Policies”.




For your convenience, there is a 'Restore Recommended' button available for restoring the default recommended settings. There are also help links on the left hand side that expand on what any individual policy does / what is enforced. There is also an 'advanced' check box that, when clicked, will grant access to advanced controls for creating your own rejection messages that should be sent when an individual policy is triggered. This is to aid in identifying your own brand and/or if you find the default rejection messages need to be tailored to your own regional locale. Please be aware that policies that are enabled at this level will **always** be checked.

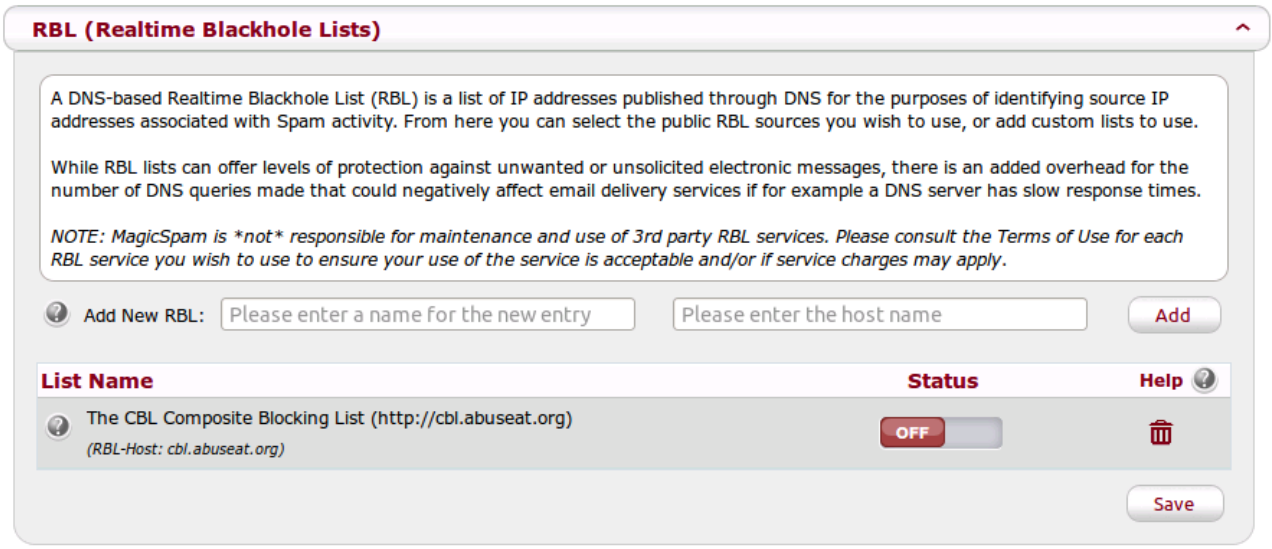
Now, click on “IP Reputation”.




There are two section available on this page. The first section is the list of BMS reputation lists. This is a high performance system of lookups designed to quickly identify and reject those sources that have a poor reputation. Similar to the server policies section, there is a 'Restore Recommended' button available for quickly restoring back to the default recommended safe set. Of Reputation lists. Please be aware that Reputation lists enabled here will **always** be checked. End customers that have a MagicSpam enabled Hosting package will be able to select additional lists that they wish to have enabled for their specific domains.

Below the BMS section there is an additional section for enabling RBL (Real time Blackhole Lists). This is to allow you to conveniently enable DNS RBLs that you may have a pre-existing subscription for.




Please note that RBL lists, unlike BMS lists, may add additional over head to mail processing as each connection and lookup requires a remote DNS lookup to be performed. These should be used sparingly. *(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).*

## Global Protection vs. Per Account Protection

There are 3 different configurations that MagicSpam PRO can be used for:

- Global protection via the WHM module. This allows the administrator of the cPanel server to set what policies to enforce and what Reputation lists should be checked.
- Per Accounts assignment. By simply disabling all policies and IP reputation lists in the WHM plugin interface, one may assign the MagicSpam resource to select Hosting packages to allow end customers to control their own spam settings.
- Combination of the above two methos is also possible. Setting server wide policies for generic global protection and allowing individual customers to control their own additional settings is the general preferred usage for MagicSpam PRO for WHM/cPanel.

## Rate Limiter Configuration

Unique to the PRO Edition of MagicSpam, there are 2 rate limiter systems included: Inbound and Outbound.

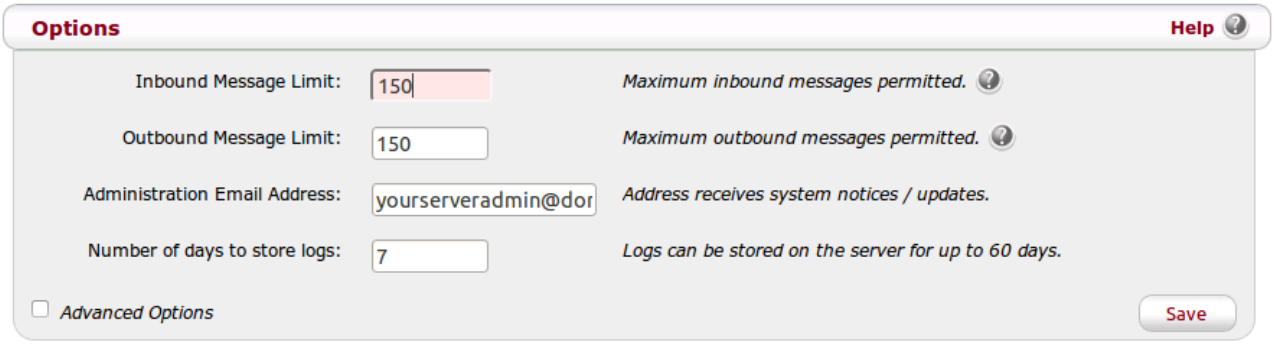
Inbound rate limiting is designed to block a particular IP address from flooding your cPanel server with an excess of attempted deliveries within a set period of time.

Outbound rate limiting is designed to block a particular customer from sending an excess

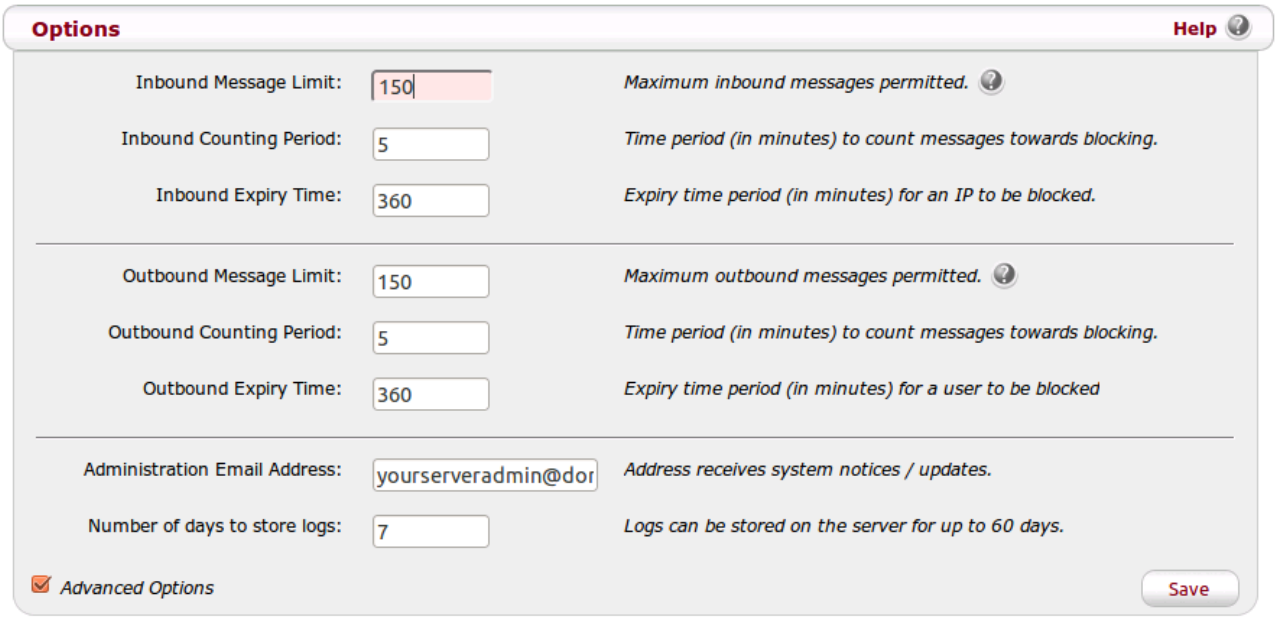
 

of messages out through your cPanel server within a set period of time, and will often act as an early indicator of a customer account password being compromised to send spam messages through your server.

The default controls for these systems are available under “Settings” / “System”.

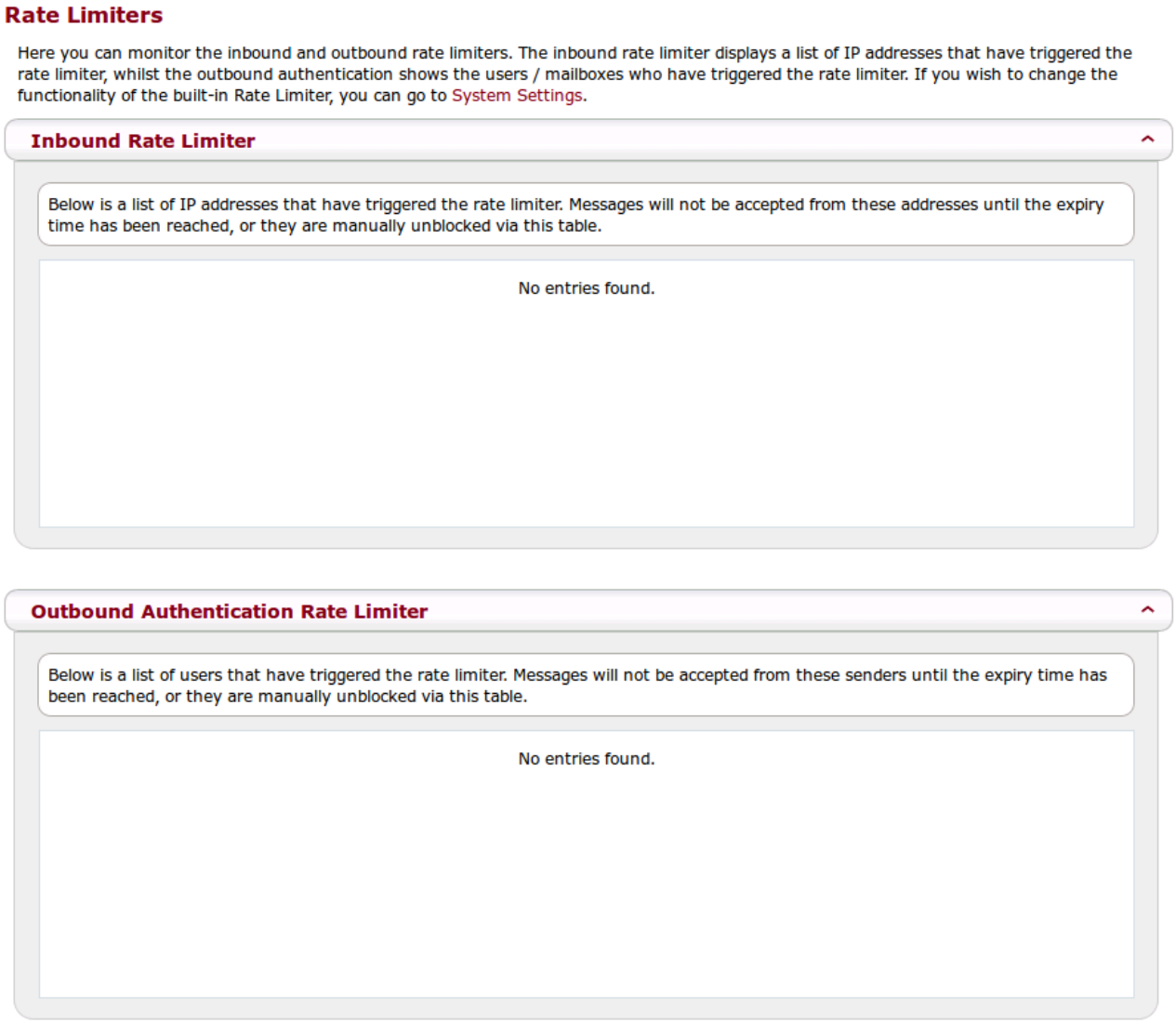



By default, MagicSpam is configured to permit up to 150 inbound messages from a remote server within a 5 minute period, and up to 150 outbound messages from a given authenticated customer within a 5 minute period. Upon triggering the 150 message limit, a given server IP OR a given customer authentication will be blocked from sending further messages for a 6 hour period. You can modify the limit by editing the values in this form. If you wish to completely disable either inbound or outbound rate limiting, simply set a value of '0' in the respective field. If you need to further fine tune the counting period or the blocking period, you can click on 'Advanced Options'.



When a given IP address OR authenticated customer triggers the rate limit, they will be blocked for the specified period of time, after which they will be automatically 'unblocked'. You have the option of unblocking them early by navigating to “Settings / Rate Limiters”.




From here you will be presented with a list of those IP addresses and/or authenticated customers that are presently blocked, details of when the block event was triggered, as well as then they will be automatically unblocked, along with an option to unblock them immediately.

Please be aware that rate limiting is global to all mail processing on the server, but you may make individual exemptions for both via “Settings / Exemptions” in the WHM interface.

This concludes the User Guide for MagicSpam PRO for WHM/cPanel. If there is anything unclear, or if you have suggestions for improvements to this guide, please feel free to let us know on the public forums at:

http://forums.magicspam.com/msprowhm