

# RedListing as a New Means to Combat Spam

MailFoundry  
December 7, 2006

## Contents

1	What is RedListing?	3
2	What impact will this have on my Mail?	3
3	What impact will this have on my MailFoundry appliance?	3
4	How do I enable RedListing?	4
5	How do I know if a server has been RedListed?	4
6	What are the RedList Settings for?	5
7	Contacting Support	5

## 1 What is RedListing?

RedListing is a technology which relies on the assumption that spammers make a number of attempts to deliver email to email addresses that do not exist.

Using this assumption, we construct a methodology for measuring the rate at which attempts are made to send emails to unknown addresses. Using said data, we can compare the rate of good attempts to bad attempts over a period of time to a user defined ratio. If the ratio of bad attempts to good attempts seen from a particular IP address exceeds the user defined ratio, that IP enters a state that is said to be “RedListed”. An IP stays RedListed for a user defined period of time and any connections or emails from that IP address is subjected to a configurable action.

## 2 What impact will this have on my Mail?

The RedListing system is designed to reduce the impact of spam by limiting the entrance of spam into the mail-flow. Once a system has been RedListed, all mail from that system is subject to the user defined action (by default a rejected connection) and usually never seen. This reduces the overall amount of spam that can enter your mailbox.

Due to the algorithms that RedListing uses, systems that are RedListed are usually systems that are part of botnets. These are machines that are running spamming software specifically for sending spam. Blocking email from these machines greatly reduces the amount of spam received.

The system should not RedList friendly email servers however, if it does happen, there is a easy way to keep it from happening by adding a whitelist (see section 5).

## 3 What impact will this have on my MailFoundry appliance?

Depending on the RedListing action that has been chosen, the impact on the MailFoundry appliance can vary greatly. Choosing “Reject Connection” for the action will improve your appliance’s performance while the other options will keep your appliances performance the way it is but still allow the reduction in spam. This can be usefull if you have a heavily loaded appliance and are looking for ways to minimize the load.

“Reject Connection”, will cause the appliance to drop the SMTP connection after sending a SMTP permanent failure level error (554). The appliance will not have to deal with a full SMTP session from RedListed hosts and will have more time to devote to processing of other email.

All other actions available through the GUI take up the same amount of processing time.

## 4 How do I enable RedListing?

Redlisting options are part of the MessageIQ system and are located under its tab in the GUI. After clicking the “MessageIQ Settings” tab at the top, you may click the “RedListing” tab on the left (this is only available if “System-wide Settings” is selected in the drop down box at the top). The RedListing options are now displayed in the main area.

First, change the “RedList check” drop-down from Disabled to Enabled.

Next, select your desired action to perform when an IP becomes RedListed. The recommended setting is “Reject Connection” under most circumstances (see Section 3) however, using the Quarantine option for a period of a week initially to test the system may be worthwhile.

Last, click Update. Changes made to the RedListing section become effective immediately.

## 5 How do I know if a server has been RedListed?

The quickest way to check the current status of a host is to use the “RedList Search” which is available in the RedListing tab under the MessageIQ Settings. Enter the IP address of the host you wish to check into the text box and click the “Search RedListed IPs” button.

If the appliance has received a connection from the host recently and RedListing is enabled, the current statistics for that IP are displayed. The “Good” field represents the number of RCPTTOs that were received from the IP that were valid within that last period of statistic collection. The “Bad” field represents the number of invalid RCPTTOs within that time period. “RedList Count” indicates the number of times in the current month that the IP address has connected to the appliance while RedListed. The column “Connection Count” represents the total number of incoming connections from the IP address to the appliance. “Percent Redlisted” is calculated from the RedList Count and the Connection Count.

The “Status” column will indicate the current status of the host as calculated using the user defined settings. Possible values in this column are “whitelisted”, “whitelisted\*\*\*”, and “redlisted”.

A whitelisted host is a host that is currently not RedListed.

A host listed as “whitelisted\*\*\*” is a host that was RedListed and the entry has now expired but, the appliance has not seen a connection from the host since the entry expired so the entry has not been reset yet.

If the host is listed as RedListed, additional information indicating the amount of time the host will remain RedListed is show in parentheses.

An “Admin Functions” column lists functions that can be quickly performed on the host. “Reset” will reset the host’s current information and change a host from RedListed to whitelisted if it is RedListed. “Whitelist” will bring the user to a whitelist entry page that is filled in with the necessary information to create

a system whitelist for the selected IP address so it will no longer be caught by a RedList.

## **6 What are the RedList Settings for?**

The RedList Settings are provided to make changes to various parts of the algorithm used in RedListing. Please contact MailFoundry support if you are having problems with RedListing before changing these settings (see Section 7).

## **7 Contacting Support**

MailFoundry Support

<http://www.mailfoundry.com/support/>

1-888-305-7776

[support@mailfoundry.com](mailto:support@mailfoundry.com)