

Local RBL Service

Introduction

A DNS-based Blackhole List (DNSBL) or Real-time Blackhole List (RBL) is a list of IP addresses which are most often used to publish the addresses of computers or networks linked to spamming; most mail server software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists.

This works pretty well for known and already categorized spammers, but what happens if a new spam campaign starts flooding your gateway as is not yet categorized?

Well in most cases the multi-layer antispam engine will block messages, but this analysis is resource intensive, and in case of a massive attack could take your server down.

Libraesva ESG offers **Local RBL Service** to protect you in these situations.

Local RBL Service is an application that runs in the background. It maintains an hourly history going back 23 hours about each IP address that sends mail through ESG.

An IP address is decided to be blocked when it has sent more than a configured number of definite spam messages in the previous 23 hours and have not sent any definite ham messages. The IP address is then put into a table of blocked IP addresses together with information when the record should expire (default after 120 hours).

Service Configuration

The service is not enabled by default, and to use it you must activate it by setting a tick next to Local RBL Service Active and selecting your daily spam threshold as follows:

Libraesva ESG Local RBL Configuration

Local RBL is service which automatically blocks threatening IP addresses, based on recent history, to prevent DoS attacks.

The service run in background and collect statistics for each message received. An IP address is decided to be blocked when it has sent more than a configured number of threat messages, and the percentage of threat messages is above the value set for threat percentage.

Not all message status are considered for blocking an IP. Definite threat are Hi-Spam, viruses, or blocked attachment, but only completely safe messages are considered clean. This leave out Spam messages, SMTP reject and other light threat, for which the block could be too aggressive.

[Service Configuration](#) [Local RBL Entries](#) [Local RBL Blacklists](#) [Local RBL Whitelists](#)

Service Configuration

☒ LocalRBL **ACTIVE**.

[Disable](#)

Settings

Message threshold:	<input type="text" value="90"/>	Minimum number of threat messages to be received before considering the threat percentage (default is 20)
Threat percentage:	<input type="text" value="90"/> %	Percentage of threat messages received compared to clean messages (Suggested is above 80%, default is 90%)
Block IP interval:	<input type="text" value="1440"/>	Minutes for which messages coming from an IP are REJECTED (default is 1440 i.e. 1 days)

[Save & Apply](#)

×**NOTE:** We recommend to start with a threshold value of 4, to avoid false positives.

Service Management

The Local RBL Service can be fully configured and managed. The administrator can check actually blocked senders, create whitelist or blacklist for the service.

You have three tabs on the main screen:

- Local RBL entries
- Local RBL blackList
- Local RBL whitelist

The **Local RBL Entries** Tab shows a list of currently blocked senders. You can see source IP, date listed and date of expire. Once expired the entry will be automatically removed and the system will start receiving email again from the sender ip. Next to each entry there are two

icons, shortcuts to whitelist or blacklist permanently the selected sender IP address.

The **Local RBL Blacklist** Tab shows blacklisted IP addresses. That means Libraesva ESG will not accept connection from these IP addresses.

The **Local RBL Whitelist** Tab shows whitelisted IP addresses, namely servers that will never be blocked by this service.