

Grey listing

General

Grey listing allows you to prevent spam by temporarily rejecting email to your server. Grey listing benefits from the fact that properly configured email servers will try to resend messages later, while spammers normally will give up immediately if your server rejects an email.

When a sender tries to deliver a message for the first time to the server, they will save the senders IP address, the senders email address and the recipient email address. This information is called a *triplet*. The mail server will reject the message and kindly ask the sending server to retry later. The next time the sending server tries to deliver an email which matches the triplet, the mail server will accept the message.

Spam messages which are stopped by grey listing are not counted in the Status page in the mail server Administrator. Also, even if you configure the mail server to deliver spam messages but modify header, messages rejected by grey listing will not be delivered due to how the grey listing mechanism work.

Minutes to defer deliver attempts

The mail server should wait 15 minutes before accepting a message.

Days before removing unused records

If the mail server temporarily rejects a message, but the sender does not try to resend the message, the mail server will remove the triplet after 5 days.

Days before removing used records

Triples exist 45 days in the mail server before there removed.

White listing

E-mail servers which uses different IP addresses every time they try to send a message to the mail server, and email servers which does not try to resend messages that has been temporarily rejected is not compatible with grey listing. We must add an IP address to such servers here. The mail server will not use grey listing for the servers. Wildcards are supported in this list