Untitled Page

Help Documentation

Greylisting

What is Greylisting and how does it work?

Greylisting is a new tool in the fight against spam. It will temporarily block incoming mail from a sender and then returns the mail to the sender's mail server with a message saying effectively, "try again later." The sending server must then retry sending the mail after the Block Period but before the Pass Period (see below for definitions of these values).

Greylisting is effective because spammers will not usually bother to attempt a second delivery, but legitimate e-mail servers will.

Why use Greylisting?

Greylisting is a very effective method of spam blocking that comes at a minimal price in terms of performance. Most of the actual processing that needs to be done for Greylisting takes place on the sender's server. It has been shown to block upwards of 95% of incoming spam simply because so many spammers don't use a standard mail server which would do automatic retries.

How do I set up Greylisting?

Note: You must be a system administrator to change Greylisting settings.

In order to set up Greylisting, click the Security button on the main toolbar, then select Greylisting from the Email Protection folder tree view.

- Block Period - The period of time (in minutes) that mail will not be accepted (default 15 minutes).
- Pass Period - The period of time (in minutes) in which the sender's mail server has to retry sending the message (default 360 minutes).
- Record Expiration - The period of time(in days) that the sender will remain immune from greylisting once it has passed (default 36 days).
- Enable Greylisting - If this is enabled it will allow Greylisting to happen.
- Enable Users to Override Greylisting - Enable this to allow users to selectively turn off Greylisting (useful if you have an account that receives time sensitive mail).
- Enable Greylisting to SmartHosts - If this feature is enabled, it will determine whether or not SmartHosts are governed by Greylisting. This is determined by evaluating the MX record of the recipient's address and matching it against the IP address of any target server IP address configured in the SmartHost settings area. For more information, see the SmarterHosts section

of the online help. System administrators should note that the following cases are exempt from Greylisting:

- Whitelisted IPs for SMTP or Greylisting
- Anyone who authenticates (includes SMTP Auth Bypass list)
- Trusted senders
- Anyone who has already sent you an email
- Any IP in the greylistBypass.xml file

Disadvantages of Greylisting

The biggest disadvantage of Greylisting is the delay of legitimate e-mail from servers not yet verified. This is especially apparent when a server attempts verify a new user's identity by sending them a confirmation email.

Some e-mail servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.