



Untitled Page

Help Documentation

Greylisting

What is Greylisting and how does it work?

Greylisting is a popular 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. As such, spam servers generally only attempt a single delivery of a spam message and don't reply to the "try again later" request.

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 icon and click Greylisting in the navigation pane. The greylisting settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- 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).
- Apply To - Select who greylisting applies to.
- Enable greylisting - Select this option to enable greylisting.
- Enable users to override greylisting - Select this option to allow users to selectively turn off greylisting (useful if you have an account that receives time sensitive mail).

- Greylist if the country for the IP address is unknown - Select this option to greylist messages when the country cannot be identified for the IP address. 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

Filters

If you set the greylisting "Apply To" setting to "Everyone except specified countries / IP addresses" then you are able to add filters based on the countries or IP addresses you want to exclude from being greylisted.

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 to 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.