Greylisting

For cPanel & WHM version 64

(*Home >> Email >> Greylisting*)

Overview

This interface allows you to configure Greylisting, a service that protects your server against unwanted email or spam. When enabled, the mail server will temporarily reject any email from a sender that the server does not recognize. If the email is legitimate, the originating server tries to send it again after a delay. After sufficient time passes, the server accepts the email.

Greylisting identifies incoming email by triplets. A triplet is a collection of three pieces of data: the IP address, the sender's address, and the recipient's address. By deferring unknown triplets, Greylisting filters spam and allows legitimate email a second chance to pass through.

Before you can access the Greylisting *Configuration Settings*, *Trusted Hosts*, and *Reports* sections of the interface, you must click *on/off* to enable the *Grey listing* feature.

Enable Greylisting

If Greylisting is disabled on the server, this interface **only** displays an *On/Off* toggle. Click the toggle to change it to *On* and enable Greylisting.

Configuration Settings

The *Configuration Settings* tab allows you to specify the Greylisting parameters.

To use Greylisting, perform the following steps:

1. Click the *Configuration Settings* tab.
2. Enter the desired values for each setting, or keep the default values.
3. Click *Save*.

The following table contains descriptions and values for the *Configuration Settings* section:

Configuration setting	Default value	Maximum value	Description
Initial Deferral Time (in minutes)	`10`	`240` (four hours)	The number of minutes during which Greylisting defers email from an unknown triplet. This time begins when the server receives the first email from an unknown IP address.
Resend Acceptance Period (in minutes)	`240`	`1440` (one day)	The number of minutes during which Greylisting accepts a resent email from an unknown triplet. This time begins when the server receives the first email from an unknown IP address.
Record Expiration Time (in minutes)	`4320`	`43200` (30 days)	The number of minutes before Greylisting deletes the triplet record and treats a resent email as though it comes from a new, unknown triplet. This time begins when the server receives the first email from an unknown IP address.

Bypass Greylisting for Hosts with Valid SPF Records	*Yes*	n/a	Whether the system automatically accepts email from hosts with a valid sender policy framework (SPF). SPF is an email validation system. It allows mail exchangers to verify whether a received mail came from a host authorized by that domain's administrators. ⚠ **Note:** On servers that run CentOS 7, you may see a `named` warning about the absence of SPF resource records on DNS. • This warning is **not** relevant on CentOS 7 servers, because RFC 7208 deprecated SPF records. CentOS 7 servers use TXT records instead of SPF records. • Red Hat 7.1 and CentOS 7.1 both contain `bind-9.9.4-23.el7`, which is an updated version of BIND that complies with RFC 7208. To resolve this issue, update your operating system to a version that contains the updated version of BIND. For more information, read the the Red Hat Bugzilla case about SPF record errors.

The following table illustrates the timeline of incoming email and Greylisting's response with the default settings:

Attempts	First resend attempt	Greylisting's response
One	n/a	• Defer email back to sender. • Add triplet to the Greylisting database.
Multiple	Within 10 minutes of initial email.	Continue to defer email back to sender until the *Initial Deferral Time* expires.
Multiple	10+ minutes after initial email.	• Deliver email to recipient. • Continue to deliver email from this triplet until the *Record Expiration Time* expires.
Multiple	240+ minutes after initial email.	Treat email as if a new, unknown triplet sent it.

Additional documentation

- Greylisting
- Common Mail Service IP Addresses
- The setup_greylist_db Script
- The manage_greylisting Script
- Configure Greylisting