Greylisting

(*WHM >> 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 *Greylisting* 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 SettingsTrusted HostsCommon Mail ProvidersReports

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 Period (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 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.

Trusted Hosts

The *Trusted Hosts* tab specifies IP addresses from which Greylisting will **not** defer email.

Add an IP address to the Trusted Hosts list

To add one or more IP addresses to the *Trusted Hosts* list, perform the following steps:

1. Select the *Trusted Hosts* tab.
2. Enter one or more IP addresses in the *New Trusted Hosts* text box.

   Notes:
   - You **must** enter each IP address or IP address range on a separate line.
   - You can enter IP addresses individually (IPv4 or IPv6), as a range, or in CIDR format.

3. Enter a comment in the *Comment* text box. This comment applies to all of the IP addresses that you add in this batch.
4. Click *Add* below the entry.

Delete an IP address from the Trusted Hosts list

To delete a single IP address from the *Trusted Hosts* list, click the *Delete* icon to the right of the IP address.

To delete multiple IP addresses from the *Trusted Hosts* list, perform the following steps:

1. Select the *Trusted Hosts* tab.
2. Select the checkboxes to the left of each IP address that you wish to remove, or select the checkbox to the left of the *Host IP Address* he ading to select them all.
3. Click the gear icon (

   

) on the top right of the list, and then select *Delete Selected*.

Note:

Select *Delete All* to remove every IP address from the *Trusted Hosts* list.

Edit comments for an IP address on the Trusted Hosts list

To edit or add a comment for an IP address on the *Trusted Hosts* list, perform the following steps:

1. Select the *Trusted Hosts* tab.
2. Click the *Edit* icon to the right of the IP address.
3. Enter a new comment in the *Comment* text box.
4. Click *Update* to save your change, or *Cancel* to reject it.

Add neighboring IP addresses to the Trusted Hosts list

Neighboring IP addresses, or netblocks, refer to the range of ARIN-assigned IP addresses that surround your server's IP address. Greylisting detects whether your server's netblock exists on the *Trusted Hosts* list. Greylisting displays a notification that allows you to add all of your netblock ranges to the *Trusted Hosts* list at the same time.

To add your neighboring IP addresses to the *Trusted Hosts* list, click *Add to Trusted Hosts* in the notification.

To add or delete your neighboring IP addresses to the *Trusted Hosts* list, perform the following steps:

1. Select the *Trusted Hosts* tab.
2. Click the gear icon (
   
) on the top right of the list.
3. Select *Add Neighboring IP Addresses* or *Remove Neighboring IP Addresses*.

Note:
Netblocks that you add through this interface automatically receive the comment: *The server's neighboring IP addresses.*

Common Mail Providers

The *Common Mail Providers* tab specifies common mail providers from which Greylisting will **not** defer mail.

Trust incoming mail from common mail providers

The majority of legitimate mail comes from well-known mail service providers. To ensure that Greylisting does not defer or delay this mail, you can choose to trust these mail providers with a few clicks rather than entering their IP addresses into the *Trusted Hosts* list.

Additionally, some mail services, such as Google Apps™, allow customers who own their own domains to relay email through their mail servers. If you select to trust the mail providers, Greylisting will not defer this mail, even if those customers' domains did not properly configure the SPF records for their mail service.

To trust new mail providers added to this list, select *Automatically trust newly added mail providers*.

To designate a mail provider as trusted, perform the following steps:

1. Select the *Common Mail Providers* tab.
2. Select the *Trust* checkbox for each mail provider you want to trust.
3. Select the *Auto Update* checkbox to automatically trust any new IP addresses assigned to that mail provider.
4. Click *Save* to implement your changes.

Click the gear icon (

) on the top right of the list to select or deselect *Trust* and *Auto Update* for all of the mail providers.

cPanel maintains the list of common mail providers based on current mail server statistics. To see the IP addresses associated with the common mail providers, read our Common Mail Service IP Addresses list.

Reports

The *Reports* tab displays information about triplets that Greylisting deferred.

The report displays the data in a user-friendly format, rounded to the nearest block of time. To see the exact date and time for any of the data, hover your pointer over each entry in the report.

Note:
Greylisting stores deferred triplet information in the Greylisting database.

- You can monitor this report to find IP addresses to add to the *Trusted Hosts* list.
- Greylisting purges records from this report every 60 minutes.
- The Greylisting database resides in the `/var/cpanel/greylist/greylist.sqlite` file.

The *Reports* tab lists the following information on deferred triplets:

Column	Description
Sender IP Address	The IP address that sent the email.
From Address	The sender's email address.
To Address	The recipient's email address.
Deferred	The number of times that Greylisting deferred the email.
Accepted	The number of times that Greylisting accepted the email.
Create Time	The date and time when Greylisting first deferred the email.
Block Expire Time	The date and time when Greylisting will stop deferring the email.
Must Retry Time	The date and time until which Greylisting will accept a resent email.
Record Expire Time	The date and time until Greylisting will remove the record from the accepted list.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

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

- The setup_greylist_db Script
- The remove_dovecot_index_files Script

- Configure Greylisting
- Email Routing
- Mail FAQ
- Mailing Lists
- Archive

- Common Mail Service IP Addresses
- Greylisting
- The manage_greylisting Script
- The setup_greylist_db Script
- How to Configure the Exim Outgoing IP Address

- UAPI Functions - cPGreyList::disable_all_domains
- WHM API 1 Functions - create_cpgreylist_trusted_host
- WHM API 1 Functions - delete_cpgreylist_trusted_host
- WHM API 1 Functions - disable_cpgreylist
- WHM API 1 Functions - enable_cpgreylist